



**UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS
CARRERA DE DERECHO**

La falta de tipificación del Ransomware y su incidencia en la desprotección de la persona jurídica.

Trabajo de titulación para optar al título de Abogada de los tribunales y juzgados de la República del Ecuador

Autora:

Huerta Morán, Estefanía

Tutor:

Dr. Diego Lenin Andrade Ulloa

Riobamba, Ecuador. 2023

DERECHOS DE AUTORÍA

Yo, Estefanía Huerta Morán, con cédula de ciudadanía 030269427-8, autora del trabajo de investigación titulado: “LA FALTA DE TIPIFICACIÓN DEL RANSOMWARE Y SU INCIDENCIA EN LA DESPROTECCIÓN DE LA PERSONA JURÍDICA”, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor de la obra referida será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 18 de diciembre de 2023.



Estefanía Huerta Morán
C.I.: 030269427-8

DICTAMEN FAVORABLE DEL TUTOR Y MIEMBROS DE TRIBUNAL

Quienes suscribimos, catedráticos designados Tutor y Miembros del Tribunal de Grado para la evaluación del trabajo de investigación “LA FALTA DE TIPIFICACIÓN DEL RANSOMWARE Y SU INCIDENCIA EN LA DESPROTECCIÓN DE LA PERSONA JURÍDICA”, presentado por Estefanía Huerta Morán, con cédula de identidad número 030269427-8, certificamos que recomendamos la APROBACIÓN de este, con fines de titulación. Previamente se ha asesorado durante el desarrollo, revisado y evaluado el trabajo de investigación escrito y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba a la fecha de su presentación.

Dr. Bécquer Carvajal.

PRESIDENTE DEL TRIBUNAL DE GRADO



Dra. Rosita Campuzano.

MIEMBRO DEL TRIBUNAL DE GRADO



Mgs. Wendy Romero.

MIEMBRO DEL TRIBUNAL DE GRADO



Dr. Diego Andrade.

TUTOR






CERTIFICADO ANTIPLAGIO

CERTIFICACIÓN

Que, **ESTEFANÍA HUERTA MORÁN** con CC: **030269427-8**, estudiante de la Carrera de **Derecho, NO VIGENTE**, Facultad de **Ciencias Políticas y Administrativas**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**La falta de tipificación del Ransomware y su incidencia en la desprotección de la persona jurídica**", cumple con el N 4%, de acuerdo al reporte del sistema Anti plagio **URKUND** porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 14 de diciembre de 2023



Dr. Diego Lenin Andrade Ulloa
TUTOR TRABAJO DE INVESTIGACIÓN

DEDICATORIA

A mis adorados padres, Mery y Raúl, quienes han sido el pilar fundamental a lo largo de mi travesía universitaria su sacrificio, esfuerzo y perseverancia han sido lecciones vivas, enseñándome la importancia de la resistencia y la capacidad de levantarme ante las adversidades. Su apoyo incondicional ha sido mi ancla durante todos estos años de formación profesional. Agradezco infinitamente su dedicación y amor que han sido la brújula que ha guiado mi camino académico. Este logro es también suyo.

A Jonathan I., el motivo detrás de mis sonrisas más sinceras y el consuelo en mis días grises, gracias por ser mi punto de confort y equilibrio cuando más lo necesito.

A mí querido sobrino Toñito, a quien agradezco por ser mi maestro en el arte de la paciencia y el amor. A mi prima Ligia, compañera incondicional que ha compartido conmigo tanto los momentos alegres como los desafíos de estos años, a cada miembro de mi familia, su presencia ha hecho cada logro más especial y cada obstáculo más superable. Gracias por ser parte esencial de mi camino.

Estefanía Huerta Morán

AGRADECIMIENTO

Agradezco a Dios por brindarme vida y salud, por permitirme compartir momentos importantes en compañía de mi familia y seres queridos.

A mis padres, quienes con su ayuda incondicional me impulsaron a cumplir con todos mis objetivos y metas.

Expreso gratitud a mí querida alma mater, Universidad Nacional de Chimborazo, así como a los docentes que desempeñaron un papel fundamental en mi formación, quienes con paciencia y amor por la enseñanza, impartieron sus conocimientos a lo largo de mi trayectoria estudiantil. Un agradecimiento especial al Dr. Diego Andrade, mi tutor, por su valiosa ayuda y acompañamiento en el desarrollo de mi trabajo de titulación. Agradezco a todos y cada uno de los miembros del departamento de Procuraduría de la UNACH por haber contribuido significativamente a mi formación preprofesional.

A cada uno de mis amigos, de manera especial a Liss, Ronny y Gabriel, agradezco por ser parte esencial de mi vida como estudiante foránea, sus locuras, consejos y sobre todo, su apoyo incondicional hicieron que me sintiera como en casa pese a estar lejos de ella, su amistad ha sido un regalo invaluable que atesoro con cariño.

Estefanía Huerta Morán.

ÍNDICE

DERECHOS DE AUTORÍA	
DICTAMEN FAVORABLE DEL TUTOR Y MIEMBROS DE TRIBUNAL	
CERTIFICADO ANTIPLAGIO	
DEDICATORIA	
AGRADECIMIENTO	
RESUMEN	
ABSTRACT	
CAPÍTULO I.....	12
INTRODUCCIÓN.....	12
PLANTEAMIENTO DEL PROBLEMA.....	13
1.1. Problema.....	13
1.2. Justificación.....	13
1.3. Objetivos.....	13
1.3.1. Objetivo General.....	13
1.3.2. Objetivos Específicos.....	13
CAPÍTULO II.....	15
MARCO TEÓRICO.....	15
2.1. Estado del arte relacionado a la temática.....	15
2.2. Aspectos teóricos.....	16
2.2.1. UNIDAD I: DELITOS INFORMÁTICOS Y RANSOMWARE.....	16
2.2.1.1. Conceptos y definiciones.....	16
2.2.1.2. Modalidad y características de los delitos informáticos.....	18
2.2.1.3. Origen y tipos de Ransomware.....	20
2.2.2 UNIDAD II: LA LEGISLACIÓN ECUATORIANA, PERUANA Y ESPAÑOLA FRENTE AL RANSOMWARE.....	23
2.2.2.1. El bien jurídico protegido en los delitos informáticos.....	23
2.2.2.2. El verbo rector en los delitos informáticos.....	25
2.2.2.3. Los sujetos del delito informático.....	26
2.2.2.4. Derecho comparado sobre la tipificación y sanción del Ransomware.....	28
2.2.3. UNIDAD III RANSOMWARE Y LA DESPROTECCIÓN DE LA PERSONA JURÍDICA.....	34
2.2.3.1. Población vulnerable a los ataques del Ransomware.....	34
2.2.3.2. Personas jurídicas como blanco de ataque del Ransomware.....	35
2.2.3.3. La desprotección de la persona jurídica frente a los ataques del Ransomware..	36
2.3 Hipótesis.....	40

CAPITULO III	41
METODOLOGÍA.....	41
3.1. Métodos	41
3.2. Enfoque de la Investigación	41
3.3. Tipo de Investigación	42
3.4. Diseño de Investigación	42
3.5. Unidad de Análisis	42
3.6. Población:	42
3.7. Muestra:	42
3.8. Técnicas de recolección de datos.....	43
3.9. Técnicas de recolección de datos.....	43
3.10. Técnicas de análisis e interpretación de la información.	43
CAPÍTULO IV	44
RESULTADOS Y DISCUSIÓN.....	44
CONCLUSIONES.....	56
RECOMENDACIONES.	57
REFERENCIAS BIBLIOGRÁFICAS	58
ANEXO 1	61
ANEXO 2	63

ÍNDICE DE GRÁFICOS.

Gráfico Nro. 1	17
Gráfico Nro. 2	20
Gráfico Nro. 3	22
Gráfico Nro. 4	27
Gráfico Nro. 5	29
Gráfico Nro. 6	33

ÍNDICE DE TABLAS

Tabla 1: Delitos informáticos	44
Tabla 2: Delitos informáticos en la legislación ecuatoriana.	45
Tabla 3: Bien jurídico protegido en los delitos informáticos	46
Tabla 4: Concepto e implicaciones legales del Ransomware.....	47
Tabla 5: Protección legal de la persona jurídica.....	48
Tabla 6: Principio de interpretación en materia penal.	49
Tabla 7: Técnicas y evolución del Ransomware	50
Tabla 8: Investigación del Ransomware.....	51
Tabla 9: Medidas de seguridad y prevención en los ataques de Ransomware.	52
Tabla 10: Recolección y preservación de evidencia digital en delitos informáticos.....	53
Tabla 11: Participación o asesoramiento en delitos informáticos.	54
Tabla 12: Leyes y regulación en materia de delitos informáticos.	55

RESUMEN

La ciberseguridad se ha convertido en un tema crítico y los delitos informáticos representan una creciente amenaza para las personas jurídicas y sus activos. El Ransomware, un software malicioso diseñado para cifrar datos y exigir un rescate, ha evolucionado como uno de los principales delitos en el ciberespacio. Esta amenaza focalizada en las personas jurídicas representa un desafío significativo debido a que los recursos financieros de las empresas se convierten en el objetivo preferido de estos ataques. La falta de legislación específica para abordar este tipo de conductas dificulta la capacidad de perseguir y procesar a los delincuentes y que, a pesar de su prevalencia, en el caso ecuatoriano no ha sido debidamente tipificado como un delito informático, generando con ello incertidumbre en el enjuiciamiento y la prevención de estos ataques. El presente estudio, a más de promover la conciencia sobre la amenaza que representa el Ransomware, analiza las implicaciones jurídicas por falta de tipificación, examinando los vacíos legales en la protección de las personas jurídicas. Se enfoca además, en la necesidad de políticas específicas que eviten la impunidad en este tipo de delitos proponiendo, a través de un estudio comparado, posibles enfoques legislativos que permitan abordar este desafío a través de una evaluación de legislación internacional que permita crear una verdadera protección legal y seguridad cibernética para las personas jurídicas.

Palabras Clave: Secuestro informático, delito informático, protección legal informática, persona jurídica.

ABSTRACT

Cybersecurity has become a critical issue, and cybercrimes pose a growing threat to legal entities and their assets. Ransomware, malicious software designed to encrypt data and demand a ransom, has evolved into one of the primary cybercrimes. This threat, specifically targeting legal entities, presents a significant challenge as the financial resources of businesses become the preferred target for these attacks. The lack of specific legislation to address such behaviors hinders the ability to pursue and prosecute offenders. Despite its prevalence, in the case of Ecuador, Ransomware has not been correctly classified as a cybercrime, creating uncertainty in the prosecution and prevention of these attacks. This study aims to raise awareness of the threat posed by Ransomware and examines the legal implications of its lack of classification. It scrutinizes the legal gaps in protecting legal entities and emphasizes the need for specific policies to prevent impunity in such crimes. Through a comparative study, the research proposes potential legislative approaches to address this challenge. By evaluating international legislation, it seeks to establish comprehensive legal protection and cybersecurity for legal entities, providing a genuine shield against these evolving threats.

Keywords: Ransomware, cybercrime, legal protection in informatics, legal entity.



Reviewed by:

Lic. Jenny Freire Rivera

ENGLISH PROFESSOR

C.C. 0604235036

CAPÍTULO I

INTRODUCCIÓN

Durante las últimas décadas, el ser humano ha experimentado un avance tecnológico inimaginable el cual ha generado la inclusión y consecuentemente el uso de herramientas tecnológicas en el desarrollo de las actividades cotidianas, facilitado de esta manera el alcance de niveles de vida nunca antes percibidos por la humanidad, sea en el ámbito laboral, social o educativo.

Si bien el devenir y la rápida evolución tecnológica han favorecido el progreso de ciertos aspectos de la vida del ser humano también ha generado necesidades jurídicas que crecen a medida que la tecnología avanza, así, el progreso trae consigo nuevas amenazas o formas de delincuencia que acechan la tranquilidad de las personas, en consecuencia, estas nuevas formas de delinquir requieren necesariamente ser regulados por el aparato judicial.

Del uso inadecuado de las tecnologías informáticas han emergido acciones ilegales que atentan contra la privacidad de la información de las personas, empresas y entidades públicas o privadas, acciones que en la mayoría de los casos tienen como finalidad la extracción, comercialización, extorsión, secuestro o daño de las bases de datos que se encuentren almacenados en los servidores personales, empresariales, o gubernamentales.

La presencia de ciberdelitos necesariamente requiere un desarrollo jurídico penal que tipifique estas conductas criminales, por lo que, resulta necesario determinar políticas específicas que regulen estas modalidades criminales. Varias legislaciones mundiales se han visto obligadas a tipificar en sus ordenamientos jurídicos estos tipos penales para evitar la impunidad en estas nuevas conductas, así que cada legislación ha dado un tratamiento diferente a los nuevos tipos penales informáticos, sea en la sanción o manera en que se cometen.

El Estado ecuatoriano no es ajeno a esta realidad, pues durante los últimos años se ha podido apreciar un creciente progreso tecnológico, es así que el desarrollo y la aparición de nuevas tecnologías han generado nuevas acciones ilícitas, las cuales requieren necesariamente acciones legales orientadas a regular este tipo de conductas, en el caso concreto del Ransomware, es un software malicioso catalogado dentro de los ciberdelitos, el cual se utiliza para secuestrar y cifrar datos personales, empresariales, estatales de los archivos del sistema operativo para posteriormente solicitar un rescate a través de criptomonedas, mismo que no se encuentra tipificado de manera específica dentro del catálogo de delitos contemplados en el Código Orgánico Integral Penal, si bien se establecen delitos contra la seguridad de los activos de los sistemas de información y comunicación, estos no tienen un enfoque netamente individualizado del delito de Ransomware como el caso de otras legislaciones, como se lo analizará posteriormente.

PLANTEAMIENTO DEL PROBLEMA

1.1.Problema

Es de conocimiento general que los delitos informáticos han aumentado en Ecuador y en todo el mundo, así que las técnicas delictivas cometidas por los ciber delincuentes han evolucionado, creando inseguridad y nuevas conductas delictivas. Es menester que la justicia actúe acorde a las necesidades de la sociedad, brindando un soporte técnico y adecuado para su juzgamiento y poder regular su conducta antijurídica.

La problemática presentada en este estudio trata sobre el secuestro de información por medio de vías informáticas, y que si bien existe una sección denominada Delitos Contra la Seguridad de Los Activos de los Sistemas de Información y Comunicación dentro del COIP, este no contempla como delito de manera singularizada al Ransomware, el cual durante los últimos años ha pasado de perturbar a equipos personales, a ser una amenaza para grandes empresas e incluso infraestructuras vitales como hospitales, bancos, compañías estatales energéticas de diferentes países incluido el Ecuador.

1.2.Justificación

La investigación planteada tiene relevancia, ya que resulta fundamental establecer un precedente que aborde esta forma de actividad delictiva denominada Ransomware y que a la actualidad impacta a la sociedad de manera general, la cual está relacionada con la manipulación y secuestro de información digital. Esto es especialmente importante debido a la ausencia de regulaciones específicas o legislación especializada que aborden el secuestro de datos mediante medios electrónicos.

Es importante destacar que la importancia de esta investigación radica en su relación con la seguridad informática y las amenazas que representa para las personas naturales, pero sobre todo para las personas jurídicas. La información obtenida se difundirá entre la población para fortalecer su seguridad integral. Además, esta investigación servirá como base para futuros estudios relacionados con el secuestro de información, también conocido como Ransomware.

1.3.Objetivos

1.3.1. Objetivo General.

Analizar si la falta de tipificación del Ransomware incide en la desprotección de la persona jurídica.

1.3.2. Objetivos Específicos.

- Conceptualizar que es el delito de Ransomware.
- Realizar un estudio del derecho comparado entre la legislación española, peruana y ecuatoriana respecto al Ransomware.

- Efectuar un análisis jurídico doctrinario sobre la desprotección de la persona jurídica en los ataques de Ransomware.

CAPÍTULO II

MARCO TEÓRICO

2.1. Estado del arte relacionado a la temática

El Ransomware durante los últimos años ha cobrado relevancia jurídica por el modo en que opera, ha pasado de afectar equipos personales a causar grandes estragos en empresas públicas y privadas del Estado, generando de esta manera una problemática jurídica que requiere regularse y así evitar posibles impunidades por este tipo de delitos relativamente nuevos dentro del ordenamiento jurídico ecuatoriano, estas conductas delictivas se comete con la finalidad de reclamar el pago de una cantidad económica a la víctima. Dentro del catálogo de delitos del COIP no existe un delito informático con características propias del Ransomware como tal, solo se prevé conductas genéricas acerca de los delitos, tras la revisión de tesis, revistas, y demás documentos informativos realizados por diferentes autores se pudo encontrar entre lo más importantes lo siguiente:

Marco Fernando Saltos Salgado, docente de la Universidad Regional Autónomas de los Andes, con sede en Santo Domingo, en el Artículo denominado Análisis conceptual del delito informático en Ecuador señala:

Para otro sector de la doctrina el delito informático tiene un contenido propio, afectando así un nuevo interés social cuyo reconocimiento legislativo urge, diferenciando así entre delitos computacionales como nuevas formas comisivas de delitos y delitos informáticos, aquellos que afectan el novísimo del bien jurídico penal propuesto (Saltos et al., 2021).

Para Fredi Gustavo Jara Cabrera en su trabajo de titulación denominado análisis de la falta de tipificación de la conducta denominada Ransomware en el COIP, establece lo siguiente:

Es menester tener presente que en nuestro ordenamiento jurídico se aplica una regla de interpretación restrictiva en la normativa penal, por lo que únicamente se sancionará al autor de una conducta si esta se encuentra tipificada con todos sus elementos, y no se castigará a una misma conducta con dos tipos penales diferentes, ya que cada tipo está creado para sancionar una sola conducta con sus variantes (Jara, 2022, p. 70).

Jorge Enrique Alvarado Chang, Licenciado en Sistemas de Información, en la Revista Científica Artistas. 2 (1), expone lo siguiente:

Cuando se habla de soberanía, se entiende que si un grupo de personas, locales o extranjeras conocidos como hackers, están ingresando sistemáticamente y sin autorización a redes informáticas de naturaleza privada o pública, entonces los organismos de seguridad y defensa, deben actuar en respuesta a esa situación de amenaza a la seguridad interna y externa, y establecer las respectivas políticas, regulaciones y

estrategias para cuidar la privacidad de las personas y la información, servicios e infraestructura sensible del Estado (Alvarado, 2020).

De acuerdo con el portal web PRIMICIAS, indica que:

El ‘Ransomware’ se vale de un programa malicioso que impide a los usuarios entrar a su sistema o a sus archivos. Luego, exige el pago de un rescate para poder acceder a ellos nuevamente. Aunque gran parte de las organizaciones no reportan extorsiones, la plataforma Ransomware, que rastrea desde hace un año los rescates, calcula que los pagos a los criminales en criptomoneda superan los USD 120 millones. De estos, casi USD 17 millones se han entregado en 2022. Para Marc Rivero, investigador de ciberseguridad de Kaspersky, esto explica el “gran avance de ese delito, puesto que puede mover más dinero que la trata de personas o la venta de armas” (Redacción Primicias , 2022).

Nuestro país no podía ser la excepción, como así lo recoge el portal Diálogo Américas, al señalar lo siguiente:

A decir de Onofa (2022), Ecuador se suma a Argentina, Brasil, Colombia, México y Perú, como uno de los países de Latinoamérica más golpeados por los delitos informáticos, principalmente códigos maliciosos (*malware*). Según el último Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, agencia de la Organización de las Naciones Unidas, Ecuador se encuentra en el puesto 119 de 182 países en vulnerabilidad por ataques cibernéticos.

“Algunas de las tácticas de los ataques incluyen el cifrado, el robo de datos, la denegación de servicio distribuida (DDoS) y el acoso, con el objetivo último de aumentar las posibilidades de cobrar (El Comercio, 2023).

2.2. Aspectos teóricos

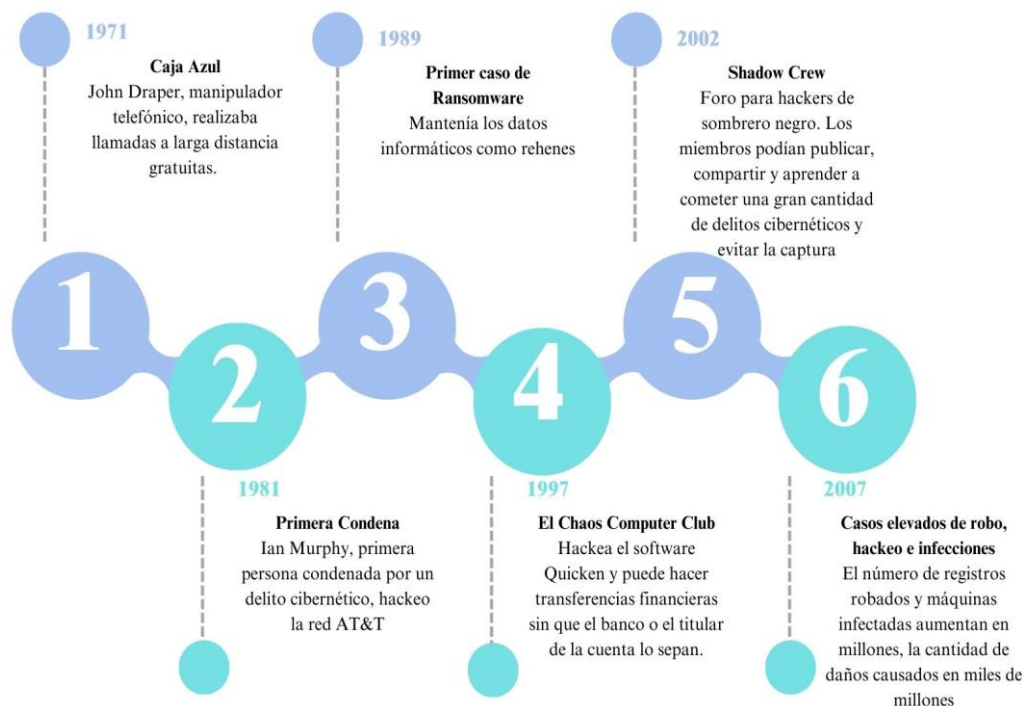
2.2.1. UNIDAD I: DELITOS INFORMÁTICOS Y RANSOMWARE.

2.2.1.1. Conceptos y definiciones

Antecedentes:

Es complejo establecer el origen de los delitos informáticos, pero se puede determinar cuáles fueron los primeros ataques que sirvieron de referencia en la evolución de los cibercrimes, así históricamente se puede referir que los delitos cibernéticos aparecieron a finales de la Segunda Guerra Mundial, pues los estados a través de las nuevas tecnologías comenzaron a atacar equipos de telecomunicaciones de otros países, en este sentido los delitos informáticos pueden rastrearse a partir de los años 60 conforme lo podemos apreciar en la línea de tiempo.

Gráfico Nro. 1
Historia abreviada de los delitos informáticos



Autora: Estefanía Huerta Morán.

Fuente: (Rinaldi, 2017)

La creación de las nuevas tecnologías sin duda alguna ha logrado una capacidad de expansión increíble, es así que el ser humano ha experimentado un avance tecnológico inimaginable que ha generado la inclusión y el uso de herramientas tecnológicas en el desarrollo de las actividades cotidianas, facilitado alcanzar niveles de vida nunca antes percibidos por la humanidad, sea en el ámbito laboral, social o educativo; la influencia que produce la tecnología en casi todas las áreas de la vida social de las personas si bien ha favorecido en el desarrollo de ciertos aspectos de la vida del ser humano también ha generado necesidades jurídicas que crecen a medida que la tecnología se desarrolla, así, el progreso trae consigo nuevas amenazas o formas de delincuencia catalogadas como delitos cibernéticos “en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad” (Casteli & Heredia, 2022).

En cuanto a delitos informáticos, una de las primeras definiciones data del año 1983, cuando la OCDE “(Organización de Cooperación y Desarrollo Económico), lo definió como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos”. (Meléndez , 2018).

En términos generales, el delito informático, cibercrimen o delito cibernético, es aquella conducta criminal que para su cometimiento requiere el uso de la tecnología como

dispositivos electrónicos e internet, en este sentido, Fuentes, Mazún y Cancino citado por (Acosta et al.,2020) lo definen como *“el conjunto de comportamientos que genera delito penal y, que debe ser tratado legalmente ya que el mismo tiene por objeto daños a terceras personas, ocasionando diferentes lesiones y, en algunos casos pérdidas de bienes jurídicos”*.

Actualmente no existe una definición propia de carácter universal respecto a los delitos informáticos, sin embargo, cabe destacar la mayoría de las definiciones atribuidas a estos ilícitos coinciden en que estos se tratan de delitos cometidos mediante el uso de sistemas, herramientas y programas informáticos como las computadoras y el internet.

Respecto al análisis precedente, cabe mencionar que los delitos informáticos desde su existencia hasta la actualidad han sido considerados como acciones ilegales que como bien se indicó en líneas anteriores para su cometimiento requieren del uso de dispositivos electrónicos e internet, cuyo objetivo es generar daños a personas y entidades vulnerando sus sistemas de seguridad, bases de datos o información de carácter sensible mediante un sinnúmero de acciones ilegales cometidas con el uso de la tecnología. Los delitos informáticos en la mayoría de los casos persiguen un beneficio económico en favor de quien o quienes los cometen, personas naturales y personas jurídicas no se encuentran exentas de ser objeto de este tipo de fechorías.

2.2.1.2. Modalidad y características de los delitos informáticos

Modalidad:

Para muchos académicos y doctrinarios la modalidad o circunstancia de un delito consiste en la forma en que se desarrolla una determinada conducta, concretamente es la manera o el modo de hacer algo de tal forma que contribuya con la caracterización de un delito, siendo estas circunstancias reproducidas por personas a lo largo del tiempo y en diferentes lugares y cuya función es determinar la pena que acarrea el cometimiento de ese delito.

Con relación a la modalidad de los delitos informáticos (Acurio del Pino , 2016, p. 11) señala que: *“el delito informático, más que una forma específica de delito supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores”*

La modalidad de los delitos informáticos no se limita, pues al existir una multiplicidad de conductas ilícitas cometidas vía informática pueden ser distintas y no sujetarse a una determinada, por lo que podemos mencionar que estas nuevas modalidades de delinquir no afectan a un bien jurídico determinado sino a una diversidad de estos.

De entre las diversas modalidades de delito informático podemos destacar las siguientes:

Pishing.- *“En cuanto al origen del término, "Phishing" resulta ser la contracción de la frase "password harvesting and fishing", que traducida al idioma castellano significa cosecha y*

pesca de contraseñas” (Oscar, 2006). Agregando a lo anterior, el Pishing suele ser considerado como una modalidad de fraude informático cuyo objetivo consiste en obtener del sujeto pasivo información sensible relacionada a los números de tarjetas de crédito, números de cuentas bancarias, contraseñas o datos de carácter personal; los sujetos activos en este delito o también conocidos como phishers simulan pertenecer a entidades bancarias o empresas de confianza mediante la duplicidad de páginas web y quienes mediante el uso de la tecnología generan enlaces, formularios, emails conducen a estas páginas web falsas, manipulando de este modo a las personas para que realicen acciones que comprometen sus datos personales.

Carding.- El carding es una modalidad de estafa cuyo objetivo es obtener los datos de las tarjetas de crédito o débito, para de esta manera falsificarlas o duplicarlas, posteriormente con toda la información sustraída los ciberdelicuentes suelen utilizar estas tarjetas para realizar compras y utilizar las tarjetas de manera no autorizada por sus titulares.

Grooming. - El grooming es otro delito informático, que opera bajo la modalidad de acoso sexual de un adulto hacia un niño, en este caso el sujeto pasivo del delito es conocido como groomer, quien bajo engaño simula ser un niño para de esta manera ganarse la confianza de sus víctimas y obtener vídeos y fotografías de carácter sexual

Doxing.-Se configura en el acto de revelar de manera intencional y pública aquella información personal de un individuo u organización sin su consentimiento, cuyo objetivo es generar daño a la trayectoria pública o profesional del individuo que sufre este tipo de ataque.

Sabotaje Informático.- El sabotaje informático es una modalidad delictiva que consiste en eliminar, modificar, suprimir funciones o datos de un computador sin autorización, con la finalidad de obstaculizar de manera intencional el correcto funcionamiento del sistema, así el sabotaje informático suele causar destrucción a los elementos físicos del sistema o destrucción de los elementos lógicos del sistema, en este primer caso se agrupan aquellas conductas orientadas a la destrucción física del sistema por ejemplo generar de manera intencional incendios, explosiones o introducción de piezas que general la cortocircuitos o demás formas de estropicio, en el segundo caso que trata de la destrucción de los elementos lógicos del sistema, este se encuentra estrechamente ligado con el uso de tecnologías informáticas que generan la destrucción, alteración de programas, bases de datos o cualquier documentación contenida en soportes electrónicos.

Espionaje informático. Consiste en el ingreso a un sistema informático ajeno para acceder y sustraer la información sensible y reservada, conocida como divulgación no autorizada de datos informáticos, utilizada en perjuicio de la víctima.

Acceso no autorizado a servicios informáticos. -

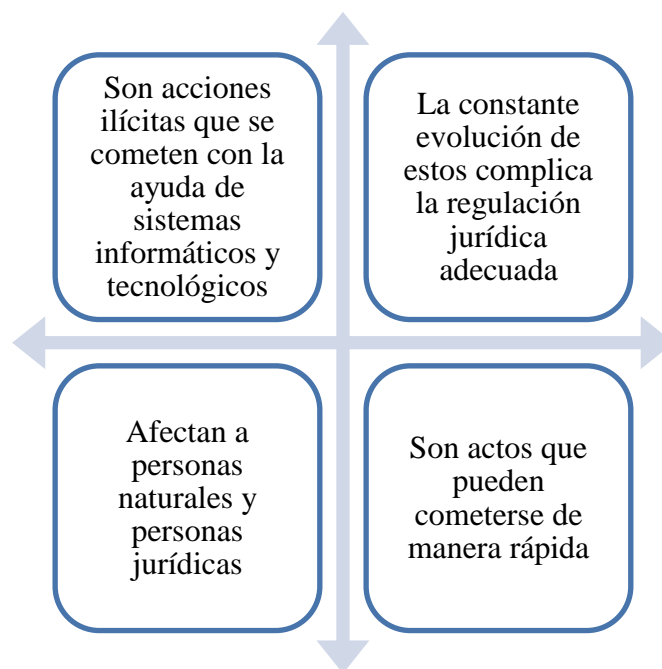
“El acceso no autorizado a un sistema informático, según los autores chilenos Marcelo Huerta y Claudio Líbano, consiste en acceder de manera indebida, sin

autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor” (Figolí, s.f.)

El acceso no autorizado a un sistema informático es un ciberdelito que consiste en la introducción a sistemas de información o computadoras vulnerando las medidas de seguridad.

Entre las características de los delitos informáticos podemos destacar las siguientes:

Gráfico Nro. 2
Características de los Delitos Informáticos



Autora: Estefanía Huerta Morán.
Fuente: (ejemplius, 2022)

2.2.1.3. Origen y tipos de Ransomware

El término Ransomware traducido de manera literal al español significa secuestro de datos, respecto a este malware existe información que en lo principal lo definen como un software malicioso que emplea el cifrado en los equipos infectados y que tiene como objetivo impedir la utilización de equipos, bloqueando o impidiendo el acceso a bases de datos, archivos, aplicaciones, ocultando información; en general mantener secuestrada la información de la víctima sea una persona en particular u organizaciones, ocurrida la infección el atacante exige el pago mediante una nota de rescate en la cual proporciona las indicaciones para que se realice el pago que generalmente es en monedas bitcoin a cambio de recuperar la clave y tener el control nuevamente del ordenador.

Conforme el párrafo anterior, el Ransomware es considerado como un programa o software dedicado al secuestro de datos o también conocido como cibersecuestro, este tipo de ataques informáticos infecta toda clase de sistemas operativos, posteriormente el atacante solicita un rescate a cambio de proporcionar nuevamente acceso a toda la información secuestrada, entre los conceptos y definiciones de algunos doctrinarios y entendidos en la materia podemos destacar la siguiente:

Trigo et al., 2017 citado por (Jara, 2022, p. 19) se conoce por Ransomware al malware o software malicioso que opera en el ordenador en el que se haya inmiscuido apoderándose de la información contenida en él y tomando control del acceso que tiene el usuario a ella, generalmente solicitando un pago como rescate de la información cifrada; en esta clase de conducta el autor del secuestro es el único que tiene conocimiento de la contraseña del cifrado, por lo que la víctima queda a total merced de su voluntad debiendo hacer lo que se le solicite si es de su deseo el obtener esta contraseña. Esta conducta tiende a evolucionar por varios factores, entre ellos la ingeniería social y las fallas detectadas por los piratas informáticos para valerse de ellas.

Desde la génesis del Ransomware han transcurrido aproximadamente 34 años, por lo que no se puede hablar del Ransomware como un tema nuevo, sin embargo, desde su creación hasta la actualidad este tipo de malware ha evolucionado hasta convertirse en grandes amenazas para las personas y empresas.

El primer Ransomware fue creado a finales de los siglos 80 por un médico estadounidense de nombres Joseph Popp y se denominó PC Ciborg o AIDS, se distribuyó 20.000 copias a 90 países mediante disquetes, el disquete contenía información educativa respecto al SIDA, sin embargo, también contenía oculto un virus que se activaba cuando el usuario reiniciaba su ordenador noventa veces.

El virus que ocultaba el disquete era un programa o software malicioso y cuando este se instalaba cifraba y encriptaba los archivos de los ordenadores y a cambio exigía el pago de un rescate para desbloquearlos, como en aquella época no existía el pago en criptomonedas, este se realizaba mediante un postal y una vez que el usuario afectado efectuara el pago este recibiría un software descifrado para que de esta manera pudiera recuperar sus archivos, si bien a inicios este tipo de malware no fue efectivo sirvió como bases para el desarrollo y creación de Ransomware más sofisticados y avanzados.

En el año 2013 apareció Cryptolocker y fue uno de los Ransomware más notorios, este se propagó con gran velocidad mediante correos electrónicos y sitios web falsos, cuando un ordenador era infectado por Cryptolocker este cifraba los archivos del usuario y solicitaba un pago a cambio de descifrarlo, el pago que podía variar conforme el plazo que el ciberdelincuente convenía. Este tipo de Ransomware más sofisticado presentaba más complicaciones para los usuarios que resultaban afectados, pues era extremadamente complicado recuperar los datos sin la clave de descifrado, convirtiéndose en el origen de Ransomwares peligrosos y más complejos.

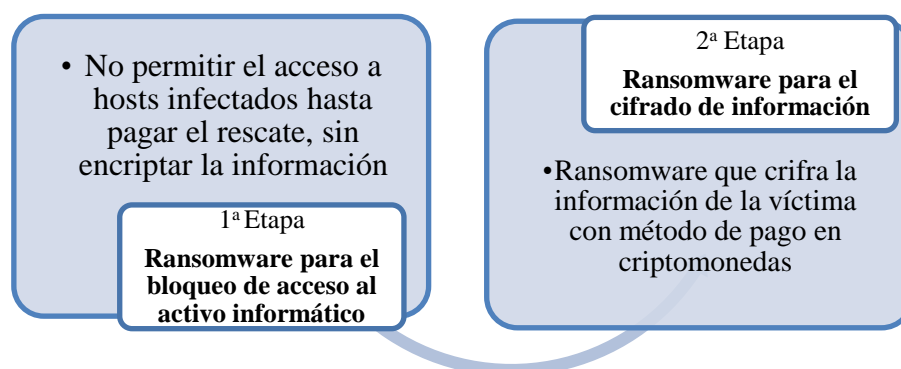
El DarkSide es otra variedad del Ransomware y una de las más actuales, se cree que sus bases se sientan en Europa el cual tiene como objetivo atacar organizaciones gubernamentales y de altos ingresos utilizando la misma modalidad del Ransomware a sus inicios, esto es el pago de un rescate, no obstante, este el DarkSide solicita un doble pago a los usuarios afectados para desbloquear los equipos afectados y para la recuperación de datos o documentos extraídos.

En el año 2021 este grupo causó un ataque contra la empresa denominada Colonial Pipeline, la cual transportaba combustible a EEUU, el ataque provocó una interrupción relevante en cuanto al suministro de combustibles, generando de esta manera graves afectaciones y consecuencias de carácter económico y social, tras dicho ataque DarkSide emitió un comunicado en el cual indicaban que su objetivo únicamente era obtener dinero y no generar daño a la sociedad.

El Ransomware sigue siendo una amenaza grave y en constante evolución, con variantes cada vez más sofisticadas y adaptadas para evadir medidas de seguridad tradicionales. En resumen, el Ransomware ha evolucionado desde sus primeras manifestaciones en la década de 1980 hasta convertirse en una amenaza cibernética seria y en constante cambio en la era moderna. Su historia refleja la adaptabilidad de los ciberdelincuentes a lo largo del tiempo y destaca la importancia de las medidas de seguridad avanzadas y la concienciación continua para combatir esta forma de ataque.

A decir de Alejandra Rodríguez Marco, en su trabajo denominado “Estudio del Impacto de un Ransomware a una PYME” previo a la obtención de su título de Máster Universitario en Ciberseguridad y Privacidad realiza la siguiente clasificación:

Gráfico Nro. 3
Etapas del Ransomware



Autora: Estefanía Huerta Morán.

Fuente: (Rodríguez, 2021, p. 14).

Actualmente el Ransomware es una de las mayores amenazas cibernéticas en auge, mismo que ha experimentado una evolución constante en sus métodos y técnicas, el cual a inicios de su creación se manifestaba principalmente a través de correos electrónicos que

engañaba a los usuarios para hacer clic en enlaces o abrir archivos maliciosos adjuntos, sin embargo con el tiempo los atacantes han perfeccionado sus tácticas utilizando exploits de software y técnicas más avanzadas de ingeniería social para filtrarse en sistemas, la propagación a través de redes también ha aumentado, afectando no solo a sistemas individuales, sino también a entornos empresariales enteros, generando impactos económicos y operativos, daños irreparables y pérdida de datos sensibles, dificultades en cuanto a la recuperación y prevención, entre otros.

2.2.2 UNIDAD II: LA LEGISLACIÓN ECUATORIANA, PERUANA Y ESPAÑOLA FRENTE AL RANSOMWARE.

2.2.2.1. El bien jurídico protegido en los delitos informáticos.

El Bien jurídico protegido

El derecho protegido, interés jurídicamente tutelado, bien garantizado, objeto de protección son sinónimo del bien jurídico protegido de un delito, conceptualmente se conoce como bien jurídico tutelado aquellos bienes materiales e inmateriales, tangibles e intangibles, cuyo valor es de suma importancia para el Estado como tal y merece la garantía de no ser vulnerado, transgredido o quebrantado por acciones u omisiones de terceros, varios estudiosos también se refieren al bien jurídico protegido como un freno ante las amenazas criminales, razón por la cual se hallan amparados por el derecho, dicho en otras palabras, el bien jurídico es *“la pretensión del legislador de darle protección a ciertos valores del ser humano”* (Zamora, 2008, p. 4).

En el caso del derecho constitucional, esta rama también tutela los bienes jurídicos, tales como el honor, la libertad, la vida, la salud entre otros; en cuanto a derecho penal nos referimos, este se limita a seleccionar ciertas conductas que lesionen o pongan en peligro los bienes jurídicos de las personas, razón por la cual el bien jurídico protegido requieren de mayor protección dado el valor que estos representan, en sentido estricto el derecho penal tiene como función esencial la protección de estos bien frente a conductas orientadas a causar daño o lesionar dichos bienes jurídicos.

En el ámbito del derecho existe el principio de exclusiva protección de bienes jurídicos, el cual señala que en el ámbito del derecho penal este debe tener como principal función la protección y el amparo de los bienes jurídicos que pudiesen ser lesionados o encontrarse en eminente peligro, para garantizar un protección efectiva de posibles vulneraciones es necesario que exista una pena orientada a prevenir la comisión de fechorías, es decir la tipificación de estas acciones ilegales, el carácter punitivo del derecho penal es el que lo diferencia de las demás ramas del derecho, es así que, el bien jurídico dentro de las ciencias penales juega un papel fundamental, pues la afectación de un bien jurídico permite determinar la sanción punitiva que esta acarrea, así mismo constituye un requisito indispensable en cuanto al ejercicio del ius puniendi de los Estados, pues permite identificar el injusto penal de los delitos, esto de conformidad a lo que indica (Carrión , 2020) *“el bien jurídico protegido a que se refiere el contenido de cada tipo penal es el elemento o aspecto*

que en la codificación moderna sirve para agrupar los delitos en los diferentes títulos del libro I del Código Orgánico Integral Penal (COIP)”.

El bien jurídico protegido en los delitos informáticos

En cuanto al bien jurídico protegido en los delitos informáticos cabe indicar que existen vertientes doctrinarias que las clasifican en dos teorías que a continuación se detallan:

Delitos informáticos que tutelan un bien jurídico específico o netamente de carácter informático. -

La primera teoría asume que los delitos informáticos tutelan un bien jurídico específico netamente diferente al que protegen aquellos delitos tradicionales, en este sentido se habla de la funcionalidad informática como el bien jurídico tutelado, entendiéndose que un software puede suministrar un correcto funcionamiento a favor de quienes emplean este tipo de tecnologías. La funcionalidad informática como bien jurídico es un término completamente nuevo a comparación de los bienes jurídicos tradicionales como el patrimonio, la intimidad, la vida y demás bienes jurídicos que afectan los delitos clásicos.

Según esta vertiente doctrinaria, la diferencia entre un delito informático y uno tradicional sería de fondo y no de forma, así que esta teoría sugiere que, en vez de modificar cuyas normas existentes, se regularán los delitos informáticos de forma independiente.

Delitos informáticos que tutelan bienes jurídicos tradicionales. -

La segunda vertiente doctrinaria contraria a la teoría ya abordada en líneas anteriores indica que, los delitos informáticos no tutelan un bien jurídico específico, pues señala que esta solo es una manera o modo delictivo que causa afectación a los bienes jurídicos tradicionales, por lo que el bien jurídico protegido en los delitos informáticos es diverso, algunos de los bienes jurídicos comúnmente protegidos en los delitos informáticos incluyen:

- a. a).- Privacidad personal y familiar.-** Los delitos contra el derecho a la intimidad personal y familiar son aquellas acciones ilícitas que tienen como objeto invadir la esfera privada de un tercero, doctrinarios señalan que el derecho a la intimidad se refiere al respeto a la personalidad humana, siendo así uno de los derechos más fundamentales del ser humano pues este protege la esfera más privada de la persona y goza de carácter reservado, por ende este derecho no se puede violentar mediante publicaciones indeseadas o sin autorización, tanto más cuando la Carta Magna en su artículo 66 establece que *“Se reconoce y garantizará a las personas: El derecho a la intimidad personal y familiar”*. (Constitución de la República del Ecuador, 2008), de igual forma el Código Orgánico Integral Penal regula este tipo de conductas, y tipifica los tipos penales que atentan contra el derecho a la privacidad como en el delito de violación a la intimidad y revelación de secreto o información personal de terceros, el COIP prevé sanciones en contra de los individuos que sin contar con la autorización legal o a su vez el consentimiento de una persona accedan, reproduzcan, difundan, publiquen datos de carácter personal o cualquier tipo de información contenida en soportes informáticos.

- b. b).- El derecho a la propiedad.-** Respecto a los delitos en contra del derecho a la propiedad, esta es una categoría de delitos que atenta contra el patrimonio de los individuos, entendiendo por patrimonio al “*Conjunto de bienes, derechos y obligaciones susceptibles de ser valoradas económicamente que pertenecen a una persona natural o jurídica*” (ACCESO A LA JUSTICIA, s.f.), en este sentido los delitos contra el derecho a la propiedad se tratan de aquellas acciones típicas que afectan o lesionan el derecho a la propiedad de una persona sobre su patrimonio, así los tipos penales tipificados dentro del COIP y que forman parte de esta categorización son: la apropiación fraudulenta por medios electrónicos, reprogramación o modificación de información de quipos terminales móviles, entre otros. ´
- c. c).- Propiedad intelectual.** - Los delitos informáticos también pueden afectar los derechos de propiedad intelectual, como el robo de propiedad intelectual, la piratería informática y la violación de derechos de autor
- d. d).- Seguridad financiera.** - La seguridad de las transacciones financieras y la protección contra fraudes cibernéticos forman parte de esta categoría, los delitos informáticos orientados al robo de información financiera o a la realización de transacciones no autorizadas afectan directamente la seguridad financiera.
- e. e).- Disponibilidad de sistemas y servicios.** - Garantizar que los sistemas informáticos estén disponibles y operativos es otro bien jurídico protegido, Los ataques de denegación de servicio y otros métodos que buscan interrumpir el funcionamiento normal de sistemas también forman parte de esta categoría.
- f. f).- Confidencialidad de la información.** - La capacidad de mantener la confidencialidad de la información es esencial. Los delitos informáticos que involucran acceso no autorizado, espionaje cibernético, robo de datos buscan violar esta confidencialidad.
- g. g).- Seguridad de la salud pública.** - En el contexto de sistemas de información de salud, la protección de datos médicos y la integridad de los registros de salud son fundamentales, los ataques que comprometen esta información pueden tener impactos directos en el sistema de salud pública.

En base a la información recabada y a todo lo expuesto, esta corriente doctrinaria manifiesta que existe amplitud en cuanto a los bienes jurídicos tutelados en el ámbito de los delitos informáticos, así también señala que la diferencia que radica en los delitos de carácter informático y aquellos delitos tradicionales es de forma y no de fondo, indicando que los delitos informáticos no tienen distinción con los demás delitos, lo cual conlleva a que para su juzgamiento no es necesaria la creación de leyes independientes sino que sugiere la modificación de leyes ya existentes para sancionar el tipo penal.

2.2.2.2. El verbo rector en los delitos informáticos.

Para Gerardo Barbosa, citado por (Rosero, 2021, p. 21) el verbo rector o principal es “*el núcleo del delito; es el comportamiento humano (acción u omisión) con la cual se lesiona el derecho de otra persona; la acción ejecutiva de cometimiento del delito, la cual generalmente está descrita por un verbo: matar, hurtar, abusar, etc*”. Conforme la cita anterior el verbo rector es la descripción de la conducta punitiva realizada por el sujeto activo

del delito el cual en la mayoría de los casos lo vamos a ubicar en el tipo penal conjugado en tercera persona del singular por ejemplo, en el delito de robo ubicamos el verbo rector en “robar”, en el delito de asesinato el verbo rector lo ubicamos en “matar”, en el caso del aborto no consentido el verbo rector lo ubicamos en “hacer abortar”, cabe indicar que al igual que los sujetos del delito el verbo rector es un elemento que nunca faltarán en el tipo penal.

Ubicar al verbo rector en infinitivo dentro de un tipo penal si bien es normal no es estrictamente obligatorio, pues existen casos en lo que ubicaremos al verbo rector con sustantivos, así por ejemplo en el delito de violación en el cual ubicamos al verbo rector en “acceso carnal”, así también se puede utilizar otra palabra o frase que si bien no es un verbo rector este hace las veces de verbo rector como por ejemplo en el delito de perjurio “faltar a la verdad”.

En cuanto al verbo rector en el contexto de los delitos informáticos cabe señalar que no hay un verbo rector único, en virtud de que los delitos informáticos pueden involucrar una variedad de acciones, de entre los verbos rectores comunes que se puede identificar en los delitos informáticos tenemos:

- ✓ Acceder: Muchos delitos informáticos conllevan el acceso no autorizado a sistemas, redes o datos.
- ✓ Interceptar: En el contexto de la interceptación de comunicaciones, algunos delitos informáticos pueden implicar la captura no autorizada de datos transmitidos
- ✓ Modificar: La alteración no autorizada de datos, sistemas o información es una acción común entre los delitos informáticos.
- ✓ Distribuir: Algunos delitos informáticos implican la distribución no autorizada de software malicioso, datos robados o información comprometida.
- ✓ Obstruir: En el caso de ataques de servicio o también conocido por sus siglas DDoS (Distributed Denial of Service), el objetivo es obstruir o interrumpir el acceso legítimo a un servicio.
- ✓ Copiar: En caso de violación de derechos de autor o robo de propiedad intelectual, el acto de copiar información sin autorización es relevante.
- ✓ Engañar: El phishing es un ejemplo de delito informático en el cual mediante el engaño a sus víctimas obtiene información confidencial

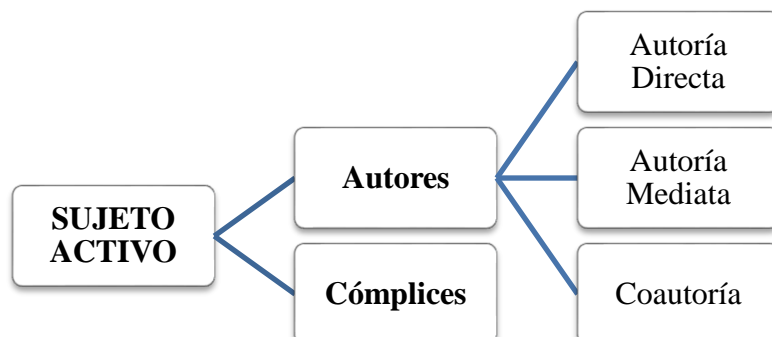
2.2.2.3. Los sujetos del delito informático.

Sujetos del delito. - Son los individuos que intervienen en la ejecución o cometimiento de un delito, el cual supone de la existencia de dos sujetos, mismos que de acuerdo a su rol se clasifican en sujeto activo y sujeto pasivo; el individuo titular del bien jurídico lesionado es el sujeto pasivo o víctima del delito, mientras que el individuo que lesione el bien jurídico protegido es denominado como sujeto activo o agresor.

Sujeto Activo. - En todos los tipos penales se distingue en primer plano el sujeto activo del delito, es decir quien efectúa o comete el delito, resulta imprescindible destacar que el sujeto activo del delito no resulta ser necesariamente quien comete el delito de manera directa y personal sino a quien pueda imputársela como un hecho propio, en el caso de la

legislación ecuatoriana las personas participan en el cometimiento de un delito conforme de detalla a continuación:

Gráfico Nro. 4
Sujetos Activos del Delito



Autora: Estefanía Huerta Morán.

Fuente: (Código Orgánico Integral Penal, 2014)

El sujeto activo a su vez se subdivide en sujeto activo calificado y sujeto activo no calificado; en este primer caso, se considera como sujeto calificado cuando requiere de determinadas características o condiciones exigibles para configurar el tipo penal, a modo de ejemplo, el Art. 278 del COIP respecto al delito de Peculado establece que los servidores públicos que abusen, distraigan o dispongan de bienes, dineros públicos y entre otros, serán sancionados con pena privativa de libertad, en este caso en concreto el sujeto activo es el servidor público, otros ejemplos con sujeto activo calificado son el delito de enriquecimiento ilícito, cohecho, concusión.

El sujeto activo no calificado por el contrario no requiere de ninguna característica en especial, en otras palabras, los delitos pueden ser cometidos por cualquier individuo sin calidad o especificidad necesaria conforme las siguientes citas:

Art. 190.- Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático (...)

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles. - La persona que intercambie (...)

Art. 230.- Interceptación ilegal de datos. - La persona que, sin orden judicial previa, en provecho propio o de un tercero intercepte, escuche, desvíe (...) (Código Orgánico Integral Penal, 2014).

En cuanto a los delitos informáticos del Código Orgánico Integral Penal, en su mayoría, los componen un sujeto activo no calificado salvo el delito tipificado en el artículo 229 respecto a la revelación ilegal de base de datos, es así que en el inciso segundo están sujetos activos calificados, siendo los servidores públicos y empleados bancarios internos.

2.2.2.4. Derecho comparado sobre la tipificación y sanción del Ransomware.

Los delitos informáticos y el Ransomware en concreto han sido objeto de estudio y análisis en varios ordenamientos jurídicos a nivel mundial, esto debido a la problemática que pueden originar en cuanto a aspectos relativos a la seguridad, privacidad y pérdidas económicas de quienes sufren este tipo de ilícitos. En muchas ocasiones resulta complejo para los países determinar responsabilidades penales por este tipo de delitos por lo que varias legislaciones se ven forzadas a recurrir a convenios internacionales y de esta manera poder regular los delitos informáticos, tal es el caso del Convenio de Budapest, el cual es considerado como un instrumento internacional precursor en la regulación de Delitos Informáticos.

El estudio comparado y el análisis entre los cuerpos legales vigentes de España, Perú y Ecuador nos permite conocer aspectos relevantes en cuanto al Ransomware, su tipificación y la incidencia en la desprotección de las personas jurídicas, así también nos permite abordar similitudes y diferencias entre las normativas legales de referidos países y de esta manera comprender los preceptos legales referentes a delitos informáticos de estos sistemas jurídicos.

Legislación Española. -

Los ataques de Ransomware a nivel mundial han incrementado de manera significativa, varias naciones se han visto perjudicadas frente a esta modalidad informática incluyendo el país europeo. Los ataques de Ransomware en este país lo ha situado entre los seis países que registra más ciberataques a nivel mundial, esto conforme datos recabados por la página web (Red Seguridad , 2023), la cual de manera textual indica lo siguiente: *“Según el informe Threat Landscape Report, elaborado por S21sec, el ransomware ha estado detrás de esta escalada de ciberataques. De hecho, ha abarcado el 65 por ciento de la totalidad de los casos detectados”*.

En el país español se ha registrado un incremento en cuanto a delitos informáticos siendo las principales víctimas de estos ilícitos las pequeñas y medianas empresas conforme la página web (Economist&Jurist, 2023). Esta manera de delinquir actualmente se ha convertido en una de las más grandes amenazas para las empresas, conforme Sophos, una empresa de ciberseguridad a nivel mundial, hace público los datos de empresas españolas atacadas por Ransomware y arroja como resultado que *“el 81% de las empresas españolas atacadas sufrió el cifrado de sus datos según revela el informe sobre “El Estado del Ransomware en España 2023” (SOPHOS NEWS, 2023), cifra relativamente alta a comparación de años anteriores.*

Legislación Penal Española. -

El Código Penal Español vigente desde el 24 de mayo de 1996 es el cuerpo normativo encargado de regular las conductas delictivas de dicho país, como dato importante cabe indicar que la legislación Española no contempla una Ley especial o autónoma respecto a los delitos informáticos, por lo que la delincuencia informática se encuentra regulada dentro de su Código Penal, sin embargo dada la necesidad de regular este tipo de conducta en el

año 2018 el Centro Criptológico Nacional del Gobierno Español desarrolla un documento denominado “Medidas de seguridad contra Ransomware”, si bien este documento de ninguna manera tipifica la conducta descrita, este establece parámetros básicos a tomarse en consideración para prevenir este tipo de ataque.

El Código Penal Español en relación al tema de estudio, incluye dentro de su catálogo de delitos las modalidades ilícitas informáticas, es así que a partir del artículo 186 tipifica los delitos informáticos, sin embargo dado el tipo de investigación es a partir del artículo 197 que se encuentran contemplados los delitos contra confidencialidad, integridad, disponibilidad de los datos y sistemas informáticos, delitos informáticos relacionados a estafas mediante manipulación informática, propiedad intelectual y derechos afines, entre otros, sin embargo la legislación penal en España no cuenta con una disposición específica que aborda directamente el Ransomware.

En el gráfico detallado se aprecia cuáles son los delitos informáticos regulados en este país.

Gráfico Nro. 5 Delitos Cibernéticos España

Art. 197.-Del descubrimiento y revelación de secretos.	<ul style="list-style-type: none">• Descubrir secretos o vulnerar la intimidad de otro sin su consentimiento, se apodere de sus papeles, cartas, correos electrónicos.• Apoderación, modificación o utilización de datos reservados personales o familiares registrados en soportes informáticos, electrónicos o telemáticos.
Art. 248.- De las estafas.	<ul style="list-style-type: none">• Los que con ánimo de lucro obstaculizan o interfirieren indebidamente en el funcionamiento de un sistema de información o alterando, borrando o suprimiendo datos informáticos
Art. 264.- Daños.	<ul style="list-style-type: none">• El que de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos, programas documentos electrónicos o informáticos.
Art. 278.- Delitos relativos al mercado y los consumidores	<ul style="list-style-type: none">• Descubrir secretos de empresa por cualquier medio de datos, documentos escritos, electrónicos, soporte informático

Autora: Estefanía Huerta Morán.

Fuente: (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal., 1995)

Si bien el Ransomware es un software latentemente peligroso para las personas y empresas, es necesario indicar que, revisada la normativa legal, de manera específica el Código Penal de esta nación, se puede apreciar que dentro del catálogo de delitos no se encuentra tipificado de manera literal el delito de Ransomware, sin embargo, se pueden apreciar otros tipos como los ya descritos el en gráfico anterior.

Revisadas las bases doctrinarias y jurisprudenciales se puede apreciar una sentencia que data del año 2016 signada con el número SAN 704/2016 - ECLI: ES: AN: 2016:704 la cual en primer aspecto trata sobre los ataques de Ransomware en la legislación española, sentencia que a continuación se detalla.

Sentencia SAN 704/2016 - ECLI: ES: AN: 2016:704

Antecedentes:

En España como consecuencia de una investigación realizada en el marco internacional contra el Ransomware se pudo determinar la afectación de más de 300 perjudicados en toda la nación Española, quienes recibieron mensajes en sus ordenadores aparentemente enviados por parte de la policía, dentro de los mensajes de texto recibidos por parte de los afectados se les hacía una advertencia de haber cometido acciones ilícitas relacionadas con la difusión de pornografía infantil, imágenes de violencia contra la integridad de menores, actos de zoofilia, así como también actos terroristas, e indicaban que para prevenir una posible difusión de todos los actos ilícitos se procedía a bloquear el sistema operativo del usuario por lo que se les solicitaban el pago de una multa equivalente a 100 euros, la misma que debía ser cancelada antes de cumplirse las 24 horas desde el momento en que el ordenador fue bloqueado pues caso contrario todos los datos serían eliminados.

En cuanto a la forma de pago a los usuarios les indicaban dos alternativas, la primera era realizar el pago mediante un cupón UKASH, el cual generalmente se utiliza para realizar compras vía internet, similar a una tarjeta de crédito solo que bajo la característica del anonimato, la segunda alternativa era realizar el pago vía paysafecard similar a la tarjeta UKASH, las mentes criminales detrás de estos ciberataques eran personas ubicadas en Rusia, quienes utilizaban foros de acceso restringido, chatas, servicios de comunicación, los miembros de estas estructuras criminales se encargaban de realizar diversas funciones entre ellas la creación y el circuito económico de este ilícito pudiendo distinguir las siguientes etapas:

- ✓ a.) Creación y distribución. - Se le denomina Ransomware Code a la persona encargada de generar, programar y poner a disposición de grupos de hackers el Ransomware, con la finalidad de obtener ganancias económicas, así también ofrecía un servicio de actualización de forma diaria para que no pudiese ser detectado por las antivirus o a su vez complicar el estudio de técnicas reversing.
- ✓ b.) Ransomware exploiters.- Son los individuos que se dedican a explotar el malware para lo cual establecen infraestructuras de dominio y servidores que facilitan la propagación e infección en los distintos ordenadores.
- ✓ c.) Infraestructura. -La contratación de los dominios al igual que el acceso a los servidores de control se mantiene en el anonimato, en esta etapa los servidores de control se encargaban de llevar el control estadístico del número de usuarios infectados, en cuanto al pago de los servicios y servidores C&C (usados en su mayoría para controlar malwares) se hacían a través de paypal o cualquier tipo de moneda electrónica.

- ✓ d.) Infección. La infección de los ordenadores es la etapa crítica, y en la mayoría de las veces se producía por navegación en internet, en páginas fraudulentas o por correos electrónicos, dado el desconocimiento de las víctimas de este ataque era imposible realizar un seguimiento adecuado de estas acciones ilícitas.
- ✓ e.) Movimiento económico del dinero obtenido. - Como bien se indicó en cuanto al rescate que estas bandas criminales solicitaban únicamente era en moneda electrónica se requería que individuos que se encarguen de convertir los códigos UKASH, PaysefeCard o Moneypak en dinero físico o virtual y de esta manera disponer de ellos.

Entre las diligencias previas realizadas se pudo conocer que existían aproximadamente 900 denuncias de personas que indicaban haber sido afectadas por Ransomware, de esta cantidad indicada 390 personas realizaron el pago que exigían los cyberdelincuentes.

Decisión del tribunal

Conforme se indicó en párrafos anteriores respecto a la tipificación del Ransomware en España no existe una norma como tal que se adecue a la conducta del Ransomware que es secuestrar datos a cambio del pago de un rescate, por lo que en la fundamentación de derecho de la presente sentencia los Magistrados indicaron que se trataba de un delito continuado de estafa, un delito de daños informáticos y un delito contra la intimidad.

Legislación Peruana

(Flores, 2023) Manifiesta que: “*Latinoamérica representó el 12% de todos los ciberataques observados, la región pasó del quinto al cuarto lugar entre las regiones más afectadas del mundo. Según el reporte del IBM Security, Perú fue uno de los países más atacados en 2022*”. Acorde a la información citada, y la investigación realizada, la modalidad del Ransomware en el País vecino no pasa por desapercibido, pues a nivel de Latinoamérica es uno de los países con más ataques de Ransomware.

Derecho Penal Peruano. -

A diferencia del país español se puede destacar que Perú cuenta con una Ley específica que regula este tipo de conductas delictivas y es la denominada Ley de Delitos Informáticos No. 30096 publicada en el año 2013, sin embargo, no siempre fue así dado que antes de la promulgación de la Ley 30096 estas conductas se regulaban dentro del Código Penal Peruano.

La Ley 30096 sienta sus bases en el Convenio sobre la Ciberdelincuencia la cual fue creada con el objeto de hacer frente a los delitos de carácter informático, actualmente esta ley sanciona las conductas ilícitas cometidas mediante el uso de tecnologías de la información que afectan sistemas, datos informáticos, entre otros bienes jurídicos, el artículo 4 de la prenombrada Ley establece lo siguiente:

Artículo 4.- Atentado contra la integridad de sistemas informáticos. - El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un

sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa. (Ley de Delitos Informáticos N°30096, 2013).

Analizado este artículo, fácilmente se podría concluir que la conducta descrita se adecua al Ransomware, pues al afectar la funcionalidad de los sistemas informáticos impidiendo, entorpeciendo el acceso o imposibilitando el funcionamiento normal este se podría considerar como un secuestro de datos, sin embargo hay que indicar el Ransomware no se configura únicamente por el secuestro de datos sino que también existe otro elemento característico de este tipo de delito y es el pago a cambio de recuperar la información secuestrada, situación que no se refleja dentro del artículo precedente.

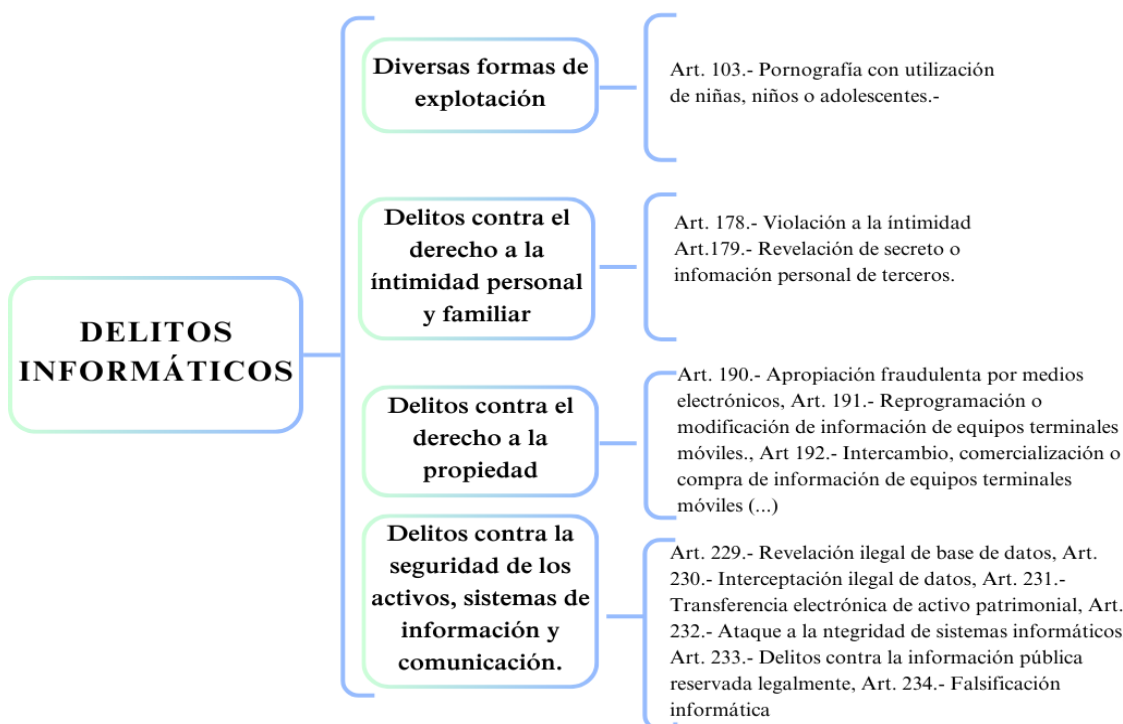
Uno de los ataques de Ransomware registrados en el vecino país ocurrió el 21 de mayo de 2022, cuando ciberdelicuentes mediante artimañas perturbaron el sistema informático de la Contraloría General de la República del Perú, tras el ataque los delincuentes hicieron pública la información obtenida, dada la poca información obtenida en relación a este caso, se desconoce cuál fue el monto solicitado por parte de los criminales a cambio de recuperar el control y la totalidad de documentos secuestrados de esta entidad pública, así como también se desconoce si en el caso en concreto existió una sentencia.

Legislación Ecuatoriana.

En la actualidad la normativa penal ecuatoriana contempla un listado de delitos informáticos tipificados dentro del Código Orgánico Integral Penal, sancionando con pena privativa de libertad aquellas conductas que involucren grabaciones, fotografías, producción, transmisión, reproducción sin consentimiento o autorización legal, suplantación de claves, utilización fraudulenta de sistemas informáticos, modificación, reprogramación de equipos terminales móviles, daños o pérdida de información de manera intencional, violación a la intimidad, a ataque a la integridad de los sistemas informáticos, acceso no consentido a sistemas informáticos entre otras acciones ilícitas relacionadas con el uso de la tecnología.

Los delitos informáticos dentro de la legislación ecuatoriana se encuentran contemplados en los siguientes artículos.

Gráfico Nro. 6
Delitos Informáticos en el COIP



Autora: Estefanía Huerta Morán.
Fuente: (Código Orgánico Integral Penal, 2014)

Partiendo desde el concepto de Ransomware, el cual opera bajo la modalidad de secuestro de datos a cambio de un pago o también conocido como cibersecuestro, el cual para Barker, citado por (Jara , 2022, p. 19) lo señala como un software “*creado con el fin de cifrar o encriptar información de instituciones y organizaciones, centrándose únicamente en la información de entidades y de empresas, con ello logrando acorralar a los directores de las mismas exigiéndoles una compensación económica como rescate*”, se puede apreciar que si bien la normativa penal ecuatoriana contempla una regulación referente a los delitos informáticos, esta no prevé una conducta literal acerca del Ransomware, pues cabe indicar que analizados los tipos penales no existe un delito que se adecue a la modalidad del Ransomware.

Ahora bien, con todo lo expuesto anteriormente resulta necesario destacar que el Código Orgánico Integral Penal en su Artículo 13 establece el principio de interpretación en materia penal, el cual señala que:

1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos.
2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma.
3. Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales

que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos. (Código Orgánico Integral Penal, 2014).

Según lo anterior, la interpretación en materia penal es una operación jurídica, es decir, que es una actividad intelectual que pretende descubrir el sentido de la norma o dicho de otra forma descubrir la voluntad de la ley para aplicarla al caso en concreto, así que la interpretación en materia penal fija estrictamente el objetivo de la norma legal, constituyéndose así en un acto de conocimiento sobre lo que la norma establece.

Por tanto, la interpretación penal es un procedimiento necesario, ya que el operador de justicia previo a la aplicación de la norma debe entender y comprender el sentido y voluntad de esta, llevar a cabo una exégesis de la norma. La interpretación de la ley en materia penal tiene relación estricta con el principio de legalidad, esto en virtud de que el derecho penal no tiene otro origen que no sea el que contempla la ley, dicho de otra manera, no existe infracción ni proceso penal sin una ley anterior a esta.

En el Ecuador la interpretación en materia penal tiene un carácter restrictivo, esto significa que: *“limita el alcance y sentido de la norma en relación con las amplias posibilidades que ofrecía su falta de precisión o su oscuridad”* (Vidaurri, 1998, p. 739), así la interpretación restrictiva le atribuye a la norma un alcance reducido.

2.2.3. UNIDAD III RANSOMWARE Y LA DESPROTECCIÓN DE LA PERSONA JURÍDICA

2.2.3.1. Población vulnerable a los ataques del Ransomware.

Los delitos informáticos y el Ransomware en general pueden afectar a cualquier usuario en particular que tenga a su alcance un ordenador o dispositivo inteligente, sin embargo, dado el avance tecnológico, las nuevas formas de delinquir y los programas más sofisticados se puede hablar de una población preferente para este tipo de delincuencia y son las empresas u organizaciones estatales o privadas independientemente de su sector, y naturaleza.

Partiendo desde un punto comparativo no es lo mismo un usuario individual que grandes organizaciones, bajo este cortejo los ciberdelicuentes buscan potenciar significativamente los beneficios que obtienen tras el ataque a un ordenador, por lo que su objetivo se centra en seleccionar víctimas con más recursos económicos y de esta manera recaudar más dinero, por ello se puede indicar cierta preferencia de los atacantes hacia las empresas y organizaciones de sectores financieros, educativos, estatales, entre otros. Pequeñas, medianas y grandes empresas a nivel mundial han sufrido ataques cibernéticos, siendo así un potencial peligro para su estructura y sus clientes.

En este punto de la investigación surge una interrogante y es ¿por qué los ciberdelicuentes dirigen sus ataques a este tipo de empresas y estructuras?, la respuesta es fácil, dada la modalidad del ransomware y al caracterizarse por exigir a las víctimas el pago

a cambio de recuperar las claves y así retomar nuevamente el control de los dispositivos hace que muchas empresas sean vulnerables a estos ilícitos, por cuanto la información que reposa en bases de datos o que se encuentra almacenada en ordenadores de dichas empresas tiene carácter de información protegida o restringida, lo cual a su vez genera que muchas empresas afectadas realicen el pago del rescate, pues en caso de que esta información fuese divulgada o en el peor de los casos que consecuencia de esta modalidad se paralicen sectores estratégicos como la salud significaría un potencial peligro para la integridad de las empresas y de sus clientes.

En relación con los párrafos anteriores, cabe mencionar que existe otro grupo vulnerable ante este tipo de ataques y son las personas físicas que por su cargo o perfil tienen bajo su poder la responsabilidad de equipos informáticos, lo cual también los hace susceptibles de sufrir estos ataques.

2.2.3.2. Personas jurídicas como blanco de ataque del Ransomware.

El Código Civil Ecuatoriano respecto a las personas jurídicas establece lo siguiente: *“Se llama persona jurídica a una persona física, capaz de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente”* (Código Civil, Asamblea Nacional, 2005). Partiendo de este precepto, una persona jurídica en el ámbito del Derecho hace referencia a un individuo con derechos y obligaciones y que si bien no existe como persona física estas existen como instituciones públicas o privadas creadas por personas físicas a las que se les reconoce una personalidad jurídica.

¿Por qué las personas jurídicas son el blanco preferido para los ataques de Ransomware?

Entendidos en el área del derecho informático indican que dada la modalidad bajo la cual opera el Ransomware resulta más probable que estas bandas ataquen entidades, empresas públicas o privadas con la finalidad de asegurarse que los pagos que exigen se realicen.

De acuerdo con Barrett, todas las instituciones están en riesgo dado el grado de sofisticación de las estructuras "ransomware-as-service (RAAS)". (Primicias , 2022). El ataque a las empresas para los ciberdelincuentes resulta más rentable que realizar ataques a individuos comunes, dentro del grupo de empresas más afectadas se puede destacar que las PYMES son un blanco de ataque fácil para los delincuentes pues al no contar con recursos económicos y de seguridad suelen ser muy vulnerables a recibir un ataque informático.

El Ransomware ha perfeccionado sus técnicas y modos de operar durante toda su trayectoria, por lo que se ha profesionalizado a nivel delictivo, expertos en ciberseguridad indican que existe tres tipos de empresas propensas a sufrir estos ataques, en primer plano se habla sobre las empresas que ya sufrieron un ataque, en segundo aspecto encontramos las empresas novatas, es decir aquellas empresas que sufrirán un ataque por primera vez y en tercer plano ubicamos la empresas que volverán a ser atacadas, muchas empresas o compañías no cuentan con las herramientas o el presupuesto necesario para prevenir y

mitigar este tipo de ataques, a nivel delictivo el Ransomware es un negocio que genera pérdidas cuantiosas a quien son víctimas de estas nuevas modalidades.

Sophos Group es una empresa que se dedica a la creación de productos de seguridad como software, hardware, conforme el informe anual publicado por Sophos se puede apreciar cuales son los desafíos que enfrentan las empresas a consecuencia del Ransomware, del total de las organizaciones encuestadas un porcentaje superior al 60% indicaron haber sido víctimas de este tipo de ataque cibernético.

Respecto al impacto empresarial que genera este malware, Sophos indica que: *“El 84 % de las organizaciones del sector privado que se han visto afectadas por un ataque de ransomware señalaron que sufrieron pérdidas de negocio/ingresos.”* (SOPHOS, 2023), el informe es claro en señalar que el Ransomware sigue siendo una gran amenaza para las empresas, la mayoría de las organizaciones seden ante los chantajes e intimidaciones de los ciberdelincuentes por lo que son más propensas a pagar el rescate.

2.2.3.3. La desprotección de la persona jurídica frente a los ataques del Ransomware.

Los ataques de Ransomware constituyen un problema serio y creciente en la actualidad, sobre todo porque dada la aparición de herramientas tecnológicas en esta era digital. El Ransomware representa una amenaza significativa para las organizaciones grandes o pequeñas, públicas o privadas, ya que puede generar pérdida de datos críticos, interrupción de las operaciones comerciales y daños financieros.

Las razones principales que contribuyen a esta desprotección incluyen:

1. Falta de legislación específica:

En algunos países la ausencia de leyes específicas que tipifiquen el Ransomware como un delito informático de manera específica implica que los perpetradores puedan eludir la responsabilidad legal de sus acciones. La falta de una base legal clara relacionada con el Ransomware puede crear lagunas en la capacidad de los organismos de aplicación de ley para perseguir y procesar a los responsables. La falta de legislación específica se presenta como un desafío clave en la lucha contra este tipo de delito informático, a continuación, se detallan algunos aspectos que incide en la falta de legislación específica:

- ✓ Complejidad y evolución del Ransomware.-La naturaleza dinámica y la constante evolución de este tipo de malware complica la adaptación de las leyes existentes para abordar y sancionar las nuevas variantes y tácticas utilizadas por los atacantes. La falta de definiciones claras y específicas dentro de los cuerpos normativos puede generar lagunas jurídicas que los delincuentes pueden aprovechar.
- ✓ Falta de sanciones adecuadas. - La falta de leyes específicas implica que las sanciones a quienes llevan a cabo ataques de Ransomware puedan no ser lo suficientemente severas como para disuadir efectivamente este tipo de actividad delictiva. La legislación existente puede no contemplar completamente la gravedad y el impacto perjudicial del Ransomware en individuos, empresas y sectores críticos.

- ✓ Colaboración Internacional. - Dado que los ataques de Ransomware a menudo trascienden las fronteras nacionales, la falta de armonización internacional en las leyes pueden dificultar la cooperación entre países para llevar a cabo investigaciones efectivas y procesar los responsables. La ausencia de estándares globales puede obstaculizar la extradición y enjuiciamiento de criminales que operan desde jurisdicciones más permisivas.
- ✓ Definición de delitos y responsabilidades. - La falta de una definición clara de lo que constituye el delito de Ransomware en la legislación puede generar una confusión en los juzgadores, fiscales, en general en los profesionales del derecho. La precisión en la redacción de las leyes es esencial para establecer responsabilidad y garantizar que los atacantes sean procesados y sancionados de manera adecuada.
- ✓ Enfoque fragmentado. - En algunos casos la legislación existente puede abordar el Ransomware indirectamente a través de disposiciones relacionadas con delitos informáticos de manera globalizada o general, sin embargo, este enfoque fragmentado puede no ser suficiente para abordar los aspectos únicos y las complejidades específicas del Ransomware, lo que destaca la necesidad de leyes que se enfoquen expresamente en este tipo de amenaza informática.

La falta de legislación específica crea un entorno legal desafiante para enfrentar el Ransomware y resalta la necesidad de reformar legales que aborden de manera adecuada esta amenaza cibernética en constante evolución. La claridad legal y la adaptabilidad a las tácticas cambiantes son esenciales para proporcionar un marco efectivo para la prevención, persecución y sanción del delito de Ransomware.

2. Desafíos técnicos: Los atacantes de Ransomware utilizan técnicas avanzadas de cifrado y suelen operar desde ubicaciones remotas o anónimas, lo que dificulta su identificación y captura.

Los desafíos técnicos en el contexto de ataques de Ransomware se refieren a las dificultades y obstáculos que enfrentan las organizaciones y profesionales de seguridad cibernética al tratar de prevenir, detectar, mitigar y recuperarse de estos ataques. Estos desafíos están vinculados a la complejidad y sofisticación de las tácticas utilizadas por los atacantes, algunos de los desafíos técnicos más prominentes se detallan a continuación.

- ✓ Cifrado avanzado. - Los atacantes de Ransomware emplean algoritmos de cifrado avanzado que dificulta la tarea de descifrar los archivos afectados sin la clave correspondiente. Este cifrado de alta complejidad no solo protege la información secuestrada, sino que también complica la capacidad de las víctimas y los expertos en seguridad para restaurar los datos.
- ✓ Operaciones desde ubicaciones remotas o anónimas. - Los perpetradores de Ransomware a menudo operan desde ubicaciones remotas o utilizan servicios para ocultar su identidad, lo que dificulta la identificación y captura de los responsables, ya que pueden aprovechar tecnologías como redes privadas y sistemas anónimos en línea.

- ✓ Uso de criptomonedas. - La mayoría de los rescates exigidos en ataques de Ransomware se solicitan las criptomonedas, como bitcoin, esta elección de monedas digitales dificulta el rastreo de las transacciones y la identificación de los destinatarios de los fondos ya que las criptomonedas ofrecen un alto grado anonimato.
- ✓ Tácticas de ingeniería social. - Muchos ataques de Ransomware se basan en tácticas de ingeniería social para engañar a los usuarios y obtener acceso a sistemas, esto puede incluir correos electrónicos de phishing, sitios web maliciosos que conllevan a la descarga e instalación de malware en los equipos informáticos.
- ✓ Desarrollo continuo de nuevas variantes. - Los atacantes están en constante evolución, creando nuevas variantes de Ransomware que pueden eludir las medidas de seguridad tradicionales, la rápida adaptación y desarrollo constante de nuevas cepas de malware presentan un desafío continuo para las soluciones de seguridad.
- ✓ Uso de herramientas legítimas. - Los atacantes a menudo aprovechan herramientas y software legítimos para facilitar sus operaciones, esto incluye el uso de herramientas administrativas y scripts que pueden pasar desapercibidos para las soluciones de seguridad, lo que complica la detección temprana de actividades maliciosas.

La combinación de estos desafíos técnicos destaca la necesidad de enfoques de seguridad proactivos y soluciones avanzadas que puedan adaptarse a las tácticas cambiantes de los ciberdelicuentes, la investigación continua y la colaboración entre la industria, los organismos gubernamentales y la comunidad de ciberseguridad son esenciales para abordar estos desafíos técnicos de manera efectiva.

3. Falta de concienciación: Muchas organizaciones y personas no están lo suficientemente informadas sobre las amenazas del Ransomware y cómo protegerse contra ellas. Esto puede hacer que sean más vulnerables a los ataques. La falta de concienciación es un desafío significativo en la lucha contra el Ransomware, la falta de comprensión y conocimiento por parte de individuos y organizaciones sobre las amenazas cibernéticas, específicamente el riesgo asociado con el Ransomware es un problema latente, algunas de los aspectos que inciden en la falta de concienciación son los siguientes:

- ✓ Desconocimiento de técnicas de ataque. - Muchas personas y empresas carecen de conocimientos detallados sobre las tácticas específicas utilizadas por los atacantes de Ransomware, esto incluye la falta de comprensión sobre cómo se propaga este malware, las formas en que los usuarios pueden ser engañados para ingresar en enlaces maliciosos y las prácticas recomendadas para evitar infecciones.
- ✓ Falta de formación en ciberseguridad. - La falta de programas educativos y de formación en ciberseguridad contribuyen a la falta de concienciación, varios usuarios y empleados no han recibido la capacitación adecuada para identificar las posibles amenazas cibernéticas, lo que los deja vulnerables al cometimiento de ciberdelitos.
- ✓ Subestimación del riesgo. - Algunas personas pueden subestimar la complejidad del Ransomware y creer que no serán blanco de un ataque, esta percepción errónea puede generar en los individuos comportamientos poco cuidadosos como la falta de

precauciones al abrir correos electrónicos sospechosos o ingresar en enlaces desconocidos.

4. **Falta de medidas de seguridad adecuadas:** Algunas organizaciones no implementan medidas de seguridad cibernética adecuadas, como copias de seguridad regulares, actualizaciones de software y capacitación del personal, lo que las deja expuestas a los ataques de Ransomware, a continuación, se detalla algunos de los fundamentales para prevenir este tipo de ataques:

- ✓ Actualización de software y sistemas. - La falta de actualización de software y sistemas operativos es una brecha común que los atacantes pueden explotar, las actualizaciones a menudo incluyen parches de seguridad que corrigen vulnerabilidad conocidas.
- ✓ Copias de seguridad insuficientes. - La falta de implementación de prácticas de copias de seguridad regulares es uno de los factores riesgos tomando en consideración que las copias de seguridad son esenciales para la recuperación de datos en caso de ataques de Ransomware, la no realización de copias de seguridad periódicas y almacenadas puede generar la pérdida de datos de manera irreversible.
- ✓ Contraseñas débiles. - La gestión deficiente de contraseñas y la falta de control sobre el acceso a sistemas y datos sensibles aumentan el riesgo de intrusiones. Las contraseñas fuertes y la autenticación de dos factores son medidas cruciales para prevenir el acceso no autorizado.
- ✓ Falta de políticas de seguridad claras. - Las organizaciones deben tener políticas de seguridad claras y aplicar medidas de cumplimiento. La ausencia de políticas específicas relacionadas con el uso seguro de sistemas y datos puede dejar a las organizaciones sin una guía clara sobre cómo prevenir y responder amenazas informáticas.

Para abordar esta desprotección, es esencial que las organizaciones tomen medidas proactivas para fortalecer su seguridad cibernética. Esto incluye implementar políticas y procedimientos de seguridad, mantener sistemas y software actualizados, realizar copias de seguridad regulares, educar al personal sobre ciberseguridad y considerar la adquisición de seguros cibernéticos para mitigar los riesgos financieros.

Además, es fundamental que los gobiernos y legisladores trabajen en la creación de marcos legales que tipifiquen el Ransomware como un delito informático y establezcan sanciones claras para los perpetradores. La cooperación internacional también desempeña un papel importante en la lucha contra el Ransomware, ya que los ciberdelincuentes a menudo operan a nivel global.

En resumen, la desprotección de las personas jurídicas frente a los ataques de Ransomware es un desafío importante, y abordarlo requiere una combinación de medidas técnicas, legales y de concienciación. La ciberseguridad se ha convertido en una prioridad crítica en el mundo actual, y la protección de datos y sistemas es esencial para el funcionamiento seguro y exitoso de las organizaciones.

2.3 Hipótesis

¿La falta de tipicidad del Ransomware incide en la desprotección de la persona jurídica?

CAPITULO III

METODOLOGÍA

La unidad de análisis se ubica en la República del Ecuador, provincia de Chimborazo, ciudad de Riobamba, espacio físico donde se aplicaron los métodos, procedimientos, técnicas, instrumentos y recursos que permitieron alcanzar los objetivos planteados.

3.1. Métodos

El problema jurídico planteado es analizado a través de los siguientes métodos:

- **Método jurídico-doctrinal:** Debido que este método permite analizar las posiciones legales sobre el tema objeto de investigación para arribar a conclusiones científicamente válidas, a través de la recolección de diversa doctrina se pudo identificar la falta de tipificación del Ransomware dentro de la legislación ecuatoriana.
- **Método jurídico-analítico:** Este método facilitó la correcta comprensión del alcance y sentido de las normas jurídicas sobre el tema a investigarse, así se identificó que, si bien el Código Orgánico Integral Penal contempla dentro de su catálogo de delitos conductas cibernéticas, este no contempla una conducta individualizada sobre el Ransomware.
- **Método inductivo:** Este método permite ejecutar el proyecto investigativo desde la práctica del pensamiento o razonamiento inductivo, caracterizado por ser ampliativo, esto a partir de una evidencia singular, que sugiere la posibilidad de una conclusión universal. Mediante este medio se buscará determinar la manera en que la falta de tipificación del Ransomware incide en la desprotección de la persona jurídica.
- **Método analítico:** Este método permitió realizar un estudio y análisis de las características del Ransomware, lo cual permitió la obtención de criterios que deriven en conclusiones específicas sobre el trabajo de investigación para determinar los efectos jurídicos que causa su falta de tipificación
- **Método descriptivo:** Mediante este método se pudo evaluar las características del Ransomware y la desprotección de las personas jurídicas, dentro de la normativa ecuatoriana.
- **Método de comparación jurídica:** Se realizó un estudio comparativo del ordenamiento jurídico nacional con la normativa legal de España y Perú para determinar la incidencia o no del Ransomware en la desprotección de la persona jurídica.

3.2. Enfoque de la Investigación

Enfoque cualitativo. – Es de enfoque cualitativo debido a que básicamente se ha indagado en definiciones, conceptos y particularidades del problema que se investigó y que versa sobre la falta de tipificación del Ransomware y su incidencia en la desprotección de la persona jurídica, tampoco se requirió de medición numérica, además se siguió un proceso

sistemático que permitió a través de un estudio jurídico, doctrinario y crítico determinar que la falta de tipificación del Ransomware incide en la desprotección de la persona jurídica.

3.3. Tipo de Investigación

Por los objetivos que se pretende alcanzar, la presente investigación es de tipo básica, documental-bibliográfica, de campo, analítica y descriptiva.

- **Básica:** La investigación es básica porque los resultados permitieron descubrir y establecer nuevos conocimientos sobre el objeto de estudio adquiridos en la investigación documental-bibliográfica.
- **Documental-bibliográfico:** Es documental-bibliográfica porque una base importante de la investigación constituyó la búsqueda bibliográfica, basada en libros, fuentes y documentos físicos o electrónicos actualizados con información científica y jurídica, además la normativa legal aplicable en el caso en concreto.
- **De campo:** La investigación es de campo debido a que la recopilación de la información concerniente al objeto de estudio se realizó en un lugar específico, en este caso, y sirvieron como base para conocer criterios legales respecto al problema jurídico planteado.
- **Descriptiva:** Mediante la investigación descriptiva y en base a los resultados obtenidos de la investigación documental bibliográfica y de campo se ha logrado describir y evaluar las características del Ransomware y la desprotección de la persona jurídica dentro de la legislación ecuatoriana.

3.4. Diseño de Investigación

Por la naturaleza y complejidad de la investigación es de diseño no experimental, porque se investigó el problema en su contexto, sin que exista manipulación intencional de variables.

3.5. Unidad de Análisis

La unidad de análisis de la presente investigación se delimita a la Provincia de Chimborazo, cantón Riobamba

3.6. Población:

La población pretende identificar los actores reales de la investigación, que aportarán con sus conocimientos desarrollando las guías metodológicas de investigación. La Población tratándose de entrevistas se enmarca en un Juez, un Fiscal y un Perito Informático

Especialistas en delitos informáticos, del cantón Riobamba, Provincia de Chimborazo.

3.7. Muestra:

En este caso se aplicó un muestreo por conveniencia de acuerdo a la facilidad de accesos y disponibilidad de las personas que formaron parte de muestra, por lo que no fue necesario extraer la muestra en vista que la población involucrada en el presente trabajo investigativo se encuentra determinada y no es extensa.

3.8. Técnicas de recolección de datos

Para obtener la información especializada referente al problema jurídico que se investigó, se utilizó la siguiente técnica e instrumento de investigación:

- Guía de entrevista

3.9. Técnicas de recolección de datos.

Para obtener la información referente al problema que se va a investigar se utilizará las siguientes técnicas e instrumentos de investigación:

Entrevista. - Es una técnica de investigación que se utiliza como instrumento de investigación al cuestionario, en el presente trabajo de investigación las entrevistas serán aplicadas a los Jueces de la Unidad Judicial Penal con sede en el Cantón Riobamba.

3.10. Técnicas de análisis e interpretación de la información.

Una vez que se recolectó la información obtenida a través de la aplicación del instrumento de investigación, se procedió al tratamiento de la información, para el procesamiento y análisis de datos se utilizará técnicas lógicas, como cuadros y gráficos estadísticos. La interpretación de los datos estadísticos se lo realizará a través de la inducción, el análisis y a la síntesis.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN.

Las entrevistas tuvieron como propósito obtener información profunda, comentada, y con un aval de veracidad, para la realización del presente proyecto investigativo, con fines eminentemente académicos y con el objetivo de contribuir a la academia, fue realizada a un Juez de la Unidad Penal, un Fiscal de FGE y un Perito Informático del cantón Riobamba, Provincia de Chimborazo.

Entrevistas dirigidas a Juez y Fiscal

Pregunta No. 1:

¿Qué son los delitos informáticos y cuáles son sus implicaciones?

Tabla 1: Delitos informáticos

ENTREVISTADO	RESPUESTA
JUEZ	Son delitos cometidos a través de sistemas informáticos, redes electrónicas u otro medio tecnológico.
FISCAL	Son aquellas acciones ilícitas cometidas mediante sistemas informáticos e internet.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

Los resultados obtenidos de la pregunta 1 permiten abordar criterios similares, pues ambos entrevistados juez y fiscal, concuerdan en que los delitos informáticos involucran acciones ilícitas cometidas a través de sistemas informáticos, lo que sugiere un entendimiento común de la esencia de estos crímenes, también son concordantes al indicar que necesariamente para el cometimiento de estas acciones se requiere del uso de las tecnologías.

De las respuestas obtenidas a esta cuestión es positivo que tanto el juez como el fiscal compartan una visión similar sobre la naturaleza de los delitos informáticos

Pregunta No. 2:
¿Cuáles son los delitos informáticos previstos en la legislación ecuatoriana?

Tabla 2: Delitos informáticos en la legislación ecuatoriana.

ENTREVISTADO	RESPUESTA
JUEZ	Entre los principales: apropiación fraudulenta por medios electrónicos, transferencia ilícita de dinero, interceptación ilegal de datos, pornografía infantil, acoso sexual, entre otros.
FISCAL	Existen varios delitos informáticos contemplados dentro de la legislación ecuatoriana como estafas, extorsiones, delitos contra la integridad sexual.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

Las respuestas obtenidas en el cuestionamiento 2 indican un consenso en la existencia y reconocimiento de delitos informáticos en la legislación ecuatoriana. Este reconocimiento abarca delitos económicos como estafas y extorsiones, así como delitos más sensibles como aquellos relacionados con la integridad sexual.

El fiscal destaca delitos económicos como estafas y extorsiones, indicando que estos están contemplados en la legislación, mientras que el juez destaca los delitos como la pornografía infantil y el acoso sexual, ambos entrevistados identifican una amplia gama de delitos informáticos en la legislación ecuatoriana, delitos que van más allá de la apropiación fraudulenta y la transferencia ilícita de dinero, incluyendo delitos como la interceptación ilegal de datos, pornografía infantil y acoso sexual.

La diversidad de delitos identificados sugiere la necesidad de que el sistema legal se adapte continuamente a los desafíos cambiantes en el ámbito de los delitos informáticos. Esto podría incluir actualizaciones legislativas para abordar nuevas formas de delitos cibernéticos.

Pregunta No. 3

¿Cuáles son los bienes jurídicos protegidos frente a los delitos informáticos?

Tabla 3: Bien jurídico protegido en los delitos informáticos

ENTREVISTADO	RESPUESTA
JUEZ	Los bienes jurídicos protegidos son la información y el patrimonio.
FISCAL	Dependiendo del delito cometido, puede ser la privacidad, el patrimonio, entre otros.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

En cuanto a las respuestas obtenidas de planteamiento 3, Ambos el juez y el fiscal coinciden en que la información y el patrimonio son bienes jurídicos protegidos en el contexto de los delitos informáticos. Esto indica una comprensión común sobre los aspectos críticos que la legislación busca salvaguardar.

El fiscal destaca que, dependiendo del delito, los bienes jurídicos protegidos pueden incluir la privacidad, el patrimonio, entre otros. Esto subraya la variabilidad y amplitud en la consideración de los bienes que pueden ser afectados por diferentes delitos informáticos.

Pregunta No. 4

¿En qué consiste el Ransomware y cuáles son sus implicaciones legales?

Tabla 4: Concepto e implicaciones legales del Ransomware

ENTREVISTADO	RESPUESTA
JUEZ	El Ransomware es una práctica ilegítima empleada por ciberdelincuentes para secuestrar datos con la intención de exigir algo a cambio para liberarlos.
FISCAL	Es un virus que bloque y sustrae datos a cambios de beneficios económicos.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

Las respuestas dadas al planteamiento número 4 evidencia un criterio y comprensión básica y concordante sobre lo que es y que implica en Ransomware. La respuesta del Juez es clara y señala al Ransomware como una práctica ilegítima utilizada por ciberdelincuentes para secuestrar datos con el propósito de exigir algo a cambio para su liberación, por su parte el Fiscal aborda el concepto de Ransomware al describirlo como un virus que bloque y sustrae los datos a cambio de beneficios económicos.

Ambas respuestas están alineadas en la comprensión de que el Ransomware implica el bloqueo y sustracción de datos con la intención de obtener beneficios económicos. Sin embargo, la respuesta del juez es más explícita al mencionar la ilegitimidad de esta práctica y la acción de exigir algo a cambio para liberar los datos.

Pregunta No. 5

¿Las normas penales existentes en Ecuador garantizan una protección eficaz a las personas jurídicas frente a delitos informáticos, como el Ransomware?

Tabla 5: Protección legal de la persona jurídica

ENTREVISTADO	RESPUESTA
JUEZ	No, por cuanto se tiene que recurrir a otras interpretaciones para proteger el bien jurídico.
FISCAL	Actualmente no existe una protección que garantice al 100% una protección eficaz para las personas jurídicas en el estado.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

Respecto a los resultados obtenidos de la pregunta número 5, las respuestas sugieren que, según la percepción de los entrevistados, la protección eficaz a las personas jurídicas frente a los delitos informáticos como el Ransomware puede no ser completa o directa a través de las normas penales existentes en Ecuador, el juzgador indica que no hay una protección eficaz proporcionada directamente por las normas penales existentes en Ecuador. Sugiere que se requieren interpretaciones adicionales o medidas complementarias para salvaguardar el bien jurídico en cuestión. Esta respuesta destaca la posible necesidad de enfoques jurídicos más amplios o modificaciones normativas para abordar completamente la protección de las personas jurídicas frente a delitos informáticos, siguiendo la misma línea el fiscal coincide con la percepción del juez al afirmar que actualmente no existe una protección que garantice al 100% la seguridad de las personas jurídicas en el estado, ambas respuestas indican una preocupación compartida sobre la efectividad de las normas penales existentes en Ecuador para proteger a las personas jurídicas contra delitos informáticos.

Pregunta No. 6

¿Cuál es su perspectiva sobre la importancia del principio de interpretación en materia penal, especialmente en lo que respecta a los delitos informáticos y el Ransomware?

Tabla 6: Principio de interpretación en materia penal.

ENTREVISTADO	RESPUESTA
JUEZ	Para mayor garantía de protección debe tipificarse el delito de Ransomware.
FISCAL	El principio de interpretación materia penal se encuentra regulado dentro del COIP en su artículo 13, y es claro al indicar que los tipos penales se interpretan al tenor literal de la norma.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

En cuanto a las respuestas obtenidas a este último planteamiento, el juez destaca la importancia de tipificar específicamente el delito de Ransomware para proporcionar una mayor garantía de protección. Esta sugerencia implica que la tipificación clara y específica de los delitos informáticos, como el Ransomware, dentro del marco legal, puede mejorar la efectividad de la protección legal, por su parte el fiscal señala que el principio de interpretación en materia penal se encuentra regulado en el Código Orgánico Integral Penal (COIP), específicamente en su artículo 13. Además, destaca que este principio establece que los tipos penales se interpretan al tenor literal de la norma. Esto indica que el fiscal enfatiza la importancia de la interpretación literal de la norma en la aplicación de la legislación penal, proporcionando así claridad y directrices precisas. Estas respuestas sugieren una preocupación por la claridad y la especificidad en la legislación relacionada con delitos informáticos, especialmente el Ransomware, la tipificación precisa de estos delitos puede ser crucial para garantizar una aplicación efectiva de la ley y una mayor protección en el ámbito legal. La referencia al principio de interpretación en el COIP destaca la importancia de seguir los lineamientos legales establecidos para garantizar una aplicación coherente y justa de la ley en este contexto.

Entrevista dirigida a Perito Informático.

Pregunta No. 1

¿Cuáles son las técnicas comunes utilizadas en los ataques de Ransomware y cómo evolucionan con el tiempo?

Tabla 7: Técnicas y evolución del Ransomware

ENTREVISTADO	RESPUESTA
PERITO INFORMÁTICO	Las técnicas comunes en los ataques de Ransomware incluyen el envío de correos electrónicos de phishing con archivos adjuntos maliciosos, la explotación de vulnerabilidades en software y sistemas desactualizados, y la propagación a través de la red. Con el tiempo, los atacantes han evolucionado hacia métodos más sofisticados, como el uso de exploits de día cero, ataques dirigidos a personas específicas (Ransomware dirigido), y la combinación de Ransomware con ataques de doble extorsión, donde se exige un rescate por la eliminación de datos robados.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

Los resultados de la pregunta número 1 en relación a las técnicas y evolución del Ransomware el perito señala que las técnicas habituales en los ataques de Ransomware abarcan el envío de correos electrónicos de phishing que contiene archivos adjuntos maliciosos, así también señala que existe explotación de vulnerabilidad en software y sistemas desactualizados. La respuesta revela la sofisticación y adaptabilidad de los atacantes de Ransomware a medida que evolucionan sus tácticas para eludir las defensas de seguridad. Los elementos clave como el phishing, la explotación de vulnerabilidades y la doble extorsión resaltan la complejidad de estos ataques. Además, la alusión a exploits de día cero y ataques dirigidos sugiere una comprensión avanzada de las tecnologías y motivaciones específicas detrás de los ataques. Este análisis puede ser valioso para la implementación de estrategias de seguridad más efectivas y la conciencia de los riesgos asociados con el Ransomware.

PREGUNTA No. 2

¿Cómo se investiga un caso de Ransomware, incluyendo la identificación de los perpetradores y la recuperación de datos?

Tabla 8: Investigación del Ransomware

ENTREVISTADO	RESPUESTA
PERITO INFORMÁTICO	La investigación de un caso de Ransomware implica el análisis forense de sistemas comprometidos para identificar la variante de Ransomware, la fuente de infección y los vectores de propagación. La identificación de los perpetradores puede ser desafiante, ya que a menudo utilizan criptomonedas para el rescate, dificultando su rastreo. La recuperación de datos generalmente implica la restauración desde copias de seguridad o, en algunos casos, la búsqueda de claves de descifrado disponibles públicamente. La colaboración con agencias de aplicación de la ley y expertos en ciberseguridad es esencial en investigaciones de Ransomware.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

La respuesta obtenida a esta interrogante es clara al destacar la importancia del análisis forense en la investigación de Ransomware, lo que incluye el análisis y examinación de sistemas comprometidos para de esta manera identificar la variante de Ransomware, la fuente de infección y los vectores, así también señala la importancia del análisis forense para comprender la naturaleza del ataque, otro aspecto a resaltar es la importancia de contar con copias de seguridad actualizadas puesto que de esta manera se puede recuperar los datos secuestrados por parte de los perpetradores.

La respuesta del perito señala la complejidad que existe en cuanto a las investigaciones en ataques de Ransomware y la importancia del análisis forense, así como las estrategias efectivas de recuperación de datos para abordar este tipo de actos.

PREGUNTA No. 3

¿Qué medidas de seguridad y prevención recomienda para proteger a las personas jurídicas y particulares de los ataques de Ransomware?

Tabla 9: Medidas de seguridad y prevención en los ataques de Ransomware.

ENTREVISTADO	RESPUESTA
PERITO INFORMÁTICO	Recomiendo medidas como la educación en seguridad cibernética para el personal, la implementación de software de seguridad actualizado, la realización regular de copias de seguridad, la segmentación de redes, la restricción de permisos, la aplicación de parches de seguridad, y la planificación de respuesta a incidentes. También es crucial tener políticas de acceso y autenticación sólidas, así como una estrategia de concienciación.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

Respecto a la pregunta 3, el perito dentro de su respuesta ofrece una visión completa sobre las medidas de seguridad y prevención recomendadas para proteger tanto a las personas jurídicas como a particulares de los ataques de Ransomware, esta respuesta abarca diversos aspectos que van desde la capacitación del personal hasta la implementación de soluciones técnicas, otro aspecto a destacar es la importancia de la educación en seguridad cibernética, el perito sugiere que los usuarios desempeñan un papel fundamental en cuanto a la prevención de los ataques, por otra parte también destaca la implementación de softwares actualizados y la necesidad de contar con soluciones tecnológicas efectivas para proteger contra posibles vulnerabilidades. En general la respuesta del perito ofrece una guía sólida y práctica para fortalecer los sistemas contra los ataques de Ransomware considerando aspectos técnicos como humanos en la estrategia de seguridad.

PREGUNTA No. 4

¿Cuál es la importancia de la recolección y preservación de evidencia digital en casos de delitos informáticos, y cómo se lleva a cabo este proceso?

Tabla 10: Recolección y preservación de evidencia digital en delitos informáticos.

ENTREVISTADO	RESPUESTA
PERITO INFORMÁTICO	La recolección y preservación de evidencia digital son fundamentales en casos de delitos informáticos, ya que proporcionan pruebas críticas. Esto se hace siguiendo procedimientos forenses digitales, utilizando herramientas especializadas para adquirir y preservar datos de manera forense, garantizando la cadena de custodia y documentando todo el proceso. Esto permite que la evidencia sea admisible en un tribunal y facilita la identificación de los responsables.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

La recolección y preservación de evidencia digital en casos de delitos informáticos son aspectos críticos para el éxito de una investigación. Estos procesos se llevan a cabo mediante procedimientos forenses digitales, utilizando herramientas especializadas para adquirir datos de manera forense. La cadena de custodia se mantiene rigurosamente para garantizar la integridad de la evidencia, y todo el proceso se documenta exhaustivamente. La importancia de estos procedimientos radica en la obtención de pruebas críticas que son admisibles en un tribunal, facilitando la identificación de los responsables del delito

PREGUNTA No. 5

¿Puede proporcionar ejemplos de casos de Ransomware o delitos informáticos que haya investigado o en los que haya proporcionado asesoramiento pericial?

Tabla 11: Participación o asesoramiento en delitos informáticos.

ENTREVISTADO	RESPUESTA
PERITO INFORMÁTICO	Como perito informático, he participado en casos de Ransomware en los que he ayudado a identificar la variante de Ransomware, evaluar el alcance del ataque y recuperar datos mediante la búsqueda de claves de descifrado. También he participado en investigaciones de fraudes informáticos, donde he rastreado transacciones sospechosas y ayudada en la identificación de los responsables.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

En cuanto a la interrogante 5, el perito informático destaca su experiencia en casos de Ransomware y fraudes informáticos, también Menciona su contribución en la identificación de variantes de Ransomware, la evaluación del alcance de los ataques y la recuperación de datos mediante la búsqueda de claves de descifrado. Además, señala su participación en investigaciones de fraudes informáticos, donde ha rastreado transacciones sospechosas y ha ayudado en la identificación de los responsables, toda esta información aportada por el perito destaca la experiencia del perito en casos prácticos, resaltando su competencia tanto en el manejo de ataques de Ransomware como en la investigación de fraudes informáticos

PREGUNTA No. 6

¿Cómo cambian las leyes y regulaciones en materia de delitos informáticos a nivel nacional, y cómo afectan a su trabajo como perito informático?

Tabla 12: Leyes y regulación en materia de delitos informáticos.

ENTREVISTADO	RESPUESTA
PERITO INFORMÁTICO	Las leyes y regulaciones en materia de delitos informáticos en la actualidad son carentes, dado que los delitos informáticos evolucionan constantemente y resulta complejo abordar nuevas amenazas cibernéticas, esta situación afecta mi trabajo como perito informático.

Fuente: Entrevista aplicada a la población involucrada en la presente investigación.

Elaborado por: Estefanía Huerta Morán.

Interpretación y discusión de resultados.

En esta última interrogante el perito informático señala que las leyes y regulaciones actuales en materia de delitos informáticos son carentes, lo que dificulta abordar las amenazas cibernéticas en constante evolución. Esta respuesta sugiere una preocupación por la falta de adaptabilidad de la legislación a los cambios rápidos en el ámbito de la ciberseguridad. Este desafío puede afectar la efectividad del trabajo del perito informático al enfrentarse a casos de delitos informático, la respuesta destaca la importancia de contar con un marco legal dinámico y actualizado para hacer frente a las cambiantes amenazas cibernéticas y garantizar la efectividad del trabajo de los expertos en ciberseguridad y peritos informáticos.

CONCLUSIONES.

- El Ransomware constituye una forma ilícita de ataque cibernético, en esencia, se trata de un tipo de software malicioso meticulosamente diseñado con el propósito de cifrar datos valiosos y, posteriormente, extorsionar a los afectados exigiendo un rescate monetario a cambio de la liberación de la información. Esta táctica, perpetrada por ciberdelincuentes altamente sofisticados, ha evolucionado de manera significativa, convirtiéndose en un flagelo para individuos y, en particular, para entidades empresariales cuyos recursos financieros se han convertido en un blanco atractivo.
- A través del estudio comparado entre la legislación española, peruana y ecuatoriana se ha podido verificar la urgencia inminente de actualizar los marcos legales en el ámbito de la ciberseguridad, la rápida evolución de las tácticas de Ransomware, caracterizada por la sofisticación constante de las técnicas empleadas por los ciberdelincuentes, subraya la necesidad imperiosa de contar con leyes que sean igualmente adaptables y dinámicas, en este contexto, la legislación actual puede quedarse rezagada frente a las innovaciones continuas en el campo del cibercrimen, lo que crea vacíos legales y dificulta la persecución efectiva de los responsables.
- El análisis jurídico doctrinario ha revelado la desprotección de las personas jurídica en los ataques de Ransomware. La falta de legislación específica y las lagunas en la protección legal destacan la urgencia de políticas y enfoques legislativos que eviten la impunidad de estos delitos cibernéticos. Este análisis ha proporcionado una visión profunda de los desafíos jurídicos que enfrentan las personas jurídicas, subrayando la necesidad de medidas preventivas y correctivas.

RECOMENDACIONES.

- Dada la creciente sofisticación del Ransomware y su impacto particularmente grave en entidades empresariales públicas y privadas, se recomienda a todas las instituciones con personería jurídica implementar y fortalecer medidas de ciberseguridad. Esto incluye la adopción de tecnologías avanzadas de detección y prevención, la realización de auditorías de seguridad de manera regular, y la inversión en la formación continua del personal en prácticas seguras en línea.
- Conforme el rápido avance de las tácticas de Ransomware y la falta de legislación específica, se recomienda a la Asamblea una revisión y actualización constante de los marcos legales relacionados con delitos cibernéticos. Estos marcos deben ser adaptables y dinámicos para abordar las innovaciones continuas en el cibercrimen. Se sugiere la implementación de la conducta Ransomware como un delito informático en el Código Orgánico Integral Penal en el que se establezcan sanciones proporcionales y faciliten la cooperación internacional para la persecución efectiva de los responsables.
- Finalmente se recomienda al Estado ecuatoriano implementar programas educativos a nivel organizacional y comunitario. Estos programas deben destacar la gravedad de las amenazas cibernéticas, proporcionar información detallada sobre las tácticas utilizadas por los ciberdelincuentes y fomentar prácticas seguras en línea. La concienciación debe ser continua y adaptarse a medida que evolucionan las amenazas cibernéticas, asegurando que las personas estén bien informadas y preparadas para enfrentar los desafíos en constante cambio del ciberespacio

REFERENCIAS BIBLIOGRÁFICAS

- ACCESO A LA JUSTICIA . (s.f.). Recuperado el 07 de Octubre de 2023, de ACCESO A LA JUSTICIA : <https://accesoalajusticia.org/glossary/patrimonio/#:~:text=Conjunto%20de%20bienes%2C%20derechos%20y,tambi%C3%A9n%20forman%20parte%20del%20patrimonio%C2%BB>.
- Acosta, M., Benavides , M., & García , N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, vol. 25, núm. 89, 2020.
- Acurio del Pino , S. (2016). Recuperado el 24 de Julio de 2023, de <http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%C3%A1ticos.%20generalidades.pdf>
- Alvarado, J. (2020). Coordinación de Investigación, Desarrollo Tecnológico e Investigación. *Revista Científica Artistas*, 75.
- Carrión , F. (02 de Septiembre de 2020). *Crónica*. Recuperado el 04 de Agosto de 2023, de Crónica: <https://cronica.com.ec/2020/09/02/el-bien-juridico-protegido/>
- Casteli, S., & Heredia, P. (17 de Agosto de 2022). *Comercio y Justicia*. Recuperado el 24 de Julio de 2023, de Comercio y Justicia: <https://comercioyjusticia.info/opinion/la-nueva-problematika-hacerles-frente-a-los-nuevos-delitos/>
- Código Civil, Asamblea Nacional. (24 de Junio de 2005). Recuperado el 03 de septiembre de 2023, de <file:///C:/Users/mega%20computers/Documents/Estefan/C%C3%B3digos/C%C3%B3digo%20Civil%20Actualizado.pdf>
- Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal*. Quito: Registro Oficial.
- Constitución de la República del Ecuador. (2008). Constitución de la República del Ecuador. *Constitución de la República del Ecuador*. Quito, Pichincha, Ecuador: Registro Oficial.
- Economist&Jurist. (3 de Enero de 2023). *Economist&Jurist*. Recuperado el 12 de Septiembre de 2023, de Economist&Jurist: <https://www.economistjurist.es/articulos-juridicos-destacados/delitos-informaticos-en-espana-estadisticas-y-como-protgerse/#:~:text=El%20Informe%20sobre%20la%20Cibercriminalidad,87%25%20son%20fraudes%20inform%C3%A1ticos>.
- ejemplius. (2022 de Febrero de 2022). *ejemplius*. Recuperado el 05 de Agosto de 2023, de ejemplius: <https://ejemplius.com/muestras-de-ensayos/delitos-informaticos-caracteristicas-y-formas-mas-comunes-en-la-que-se-cometen/>
- El Comercio. (22 de Marzo de 2023). *El Comercio*. Recuperado el 29 de Abril de 2023, de El Comercio: <https://elcomercio.pe/tecnologia/ciberseguridad/los-ataques-de-ransomware-hacia-empresas-de-latinoamerica-aumentaron-en-un-38-segun-informe-ciberseguridad-espana-mexico-colombia-noticia/>

- Figolí Pacheco, A. (s.f.). *VLEX*. Recuperado el 04 de Agosto de 2023, de VLEX: <https://vlex.es/vid/acceso-autorizado-sistemas-informaticos-107447>
- Flores, H. (1 de Marzo de 2023). *ForbesPerú*. Recuperado el 30 de Septiembre de 2023, de ForbesPerú: <https://forbes.pe/tecnologia/2023-03-01/estudio-peru-fue-uno-de-los-paises-que-registro-mas-ciberataques-de-america-latina-en-2022>
- Jara Cabrera , F. (2022). ANÁLISIS DE LA FALTA DE TIPIFICACIÓN DE LA CONDUCTA RANSOMWARE EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL. *ANÁLISIS DE LA FALTA DE TIPIFICACIÓN DE LA CONDUCTA RANSOMWARE EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL*. Cuenca, Azuay, Ecuador: Universidad Católica de Cuenca.
- Jara, F. (2022). Recuperado el 17 de Julio de 2023, de <https://dspace.ucacue.edu.ec/bitstream/ucacue/13332/1/TESIS%20FREDI%20GUSTAVO%20JARA%20CABRERA.pdf>
- Ley de Delitos Informáticos N°30096. (2013). Recuperado el 02 de Septiembre de 2023, de [https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCC F05258316006064AB/\\$FILE/6_Ley_30096.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCC F05258316006064AB/$FILE/6_Ley_30096.pdf)
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (1995). Recuperado el 02 de Septiembre de 2023, de <file:///F:/Tesis,%20Bibliograf%C3%ADa/C%C3%B3digo%20Penal%20Espa%C3%B1ol.pdf>
- Meléndez , J. (25 de junio de 2018). *DerechoEcuador.com*. Recuperado el 24 de Julio de 2023, de DerechoEcuador.com: <https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/>
- Onofa , M. (30 de Junio de 2022). *Diálogo Américas*. Recuperado el 29 de Abril de 2023, de Diálogo Américas: <https://dialogo-americas.com/es/articulos/ataques-ciberneticos-amenazan-seguridad-en-ecuador/#.ZE3NInZBzIU>
- Oscar, S. (2006). *SAIJ*. Recuperado el 04 de Agosto de 2023, de SAIJ: http://www.saij.gob.ar/doctrina/dacf060096-bisquert-figura_phishing_como_modalidad.htm
- Primicias . (12 de Junio de 2022). *Primicias* . Recuperado el Septiembre de 03 de 2023, de Primicias : <https://www.primicias.ec/noticias/tecnologia/ransomware-acecha-ecuador-paises-region/>
- Red Seguridad . (28 de Febrero de 2023). *Red Seguridad*. Recuperado el 13 de Septiembre de 2023, de Red Seguridad: https://www.redseguridad.com/actualidad/ciberdelitos/el-ransomware-situa-a-espana-entre-los-seis-paises-mas-ciberatacados-del-mundo_20230228.html
- Redacción Primicias . (12 de Junio de 2022). *PRIMICIAS* . Recuperado el 29 de Abril de 2023, de PRIMICIAS : <https://www.primicias.ec/noticias/tecnologia/ransomware-acecha-ecuador-paises-region/>
- Rinaldi, P. (27 de Abril de 2017). *LE VPN*. Recuperado el 16 de Julio de 2023, de LE VPN: <https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/>
- Rodríguez Marco, A. (Diciembre de 2021). *Estudio del impacto de un Ransomware a una PYME*. Recuperado el 28 de septiembre de 2023, de Estudio del impacto de un Ransomware a una PYME:

- <https://openaccess.uoc.edu/bitstream/10609/137992/6/aroDRiguezmarcoTFM1221memoria.pdf>
- Rosero Altamirano, M. (2021). Recuperado el 23 de Septiembre de 2023, de <http://dspace.unach.edu.ec/bitstream/51000/8033/1/5.-TESIS%20ABIGAIL%20ROSERO-DER.pdf>
- Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Scielo*.
- SOPHOS. (2023). *SOPHOS*. Recuperado el 4 de Septiembre de 2023, de SOPHOS: <file:///F:/Tesis,%20Bibliograf%C3%ADa/sophos-state-of-ransomware-2023-wpes.pdf>
- SOPHOS NEWS. (21 de Junio de 2023). *SOPHOS NEWS*. Recuperado el 13 de Septiembre de 2023, de SOPHOS NEWS: <https://news.sophos.com/es-es/2023/06/21/las-empresas-espanolas-son-cada-vez-mas-vulnerables-al-cifrado-de-datos-en-un-ataque-de-ransomware-por-encima-de-la-media-mundial/>
- Vidaurri Arechiga, M. (1998). La interpretación de la ley penal. *La interpretación de la ley penal*. México: Universidad Nacional Autónoma de México.
- Zamora Jiménez, A. (2008). *BIEN JURÍDICO Y CONSENTIMIENTO EN DERECHO PENAL*. Recuperado el 22 de Septiembre de 2023, de BIEN JURÍDICO Y CONSENTIMIENTO EN DERECHO PENAL: https://cuci.udg.mx/sites/default/files/bien_juridico.pdf

ANEXO 1

UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE CIENCIAS
POLÍTICAS Y ADMINISTRATIVAS
CARRERA DE DERECHO



GUÍA DE ENTREVISTA

Fecha: _____

Hora: _____

Lugar (ciudad y sitio específico): _____

Entrevistador: Huerta Morán Estefanía

Entrevistado (a): _____

Introducción: La presente entrevista está dirigida a Jueces Penales, Fiscales, Abogados y Peritos Informáticos de la Ciudad de Riobamba, Provincia de Chimborazo y tiene por objeto recabar información para la realización del Proyecto de Investigación titulado “**LA FALTA DE TIPIFICACIÓN DEL RANSOMWARE Y SU INCIDENCIA EN LA DESPROTECCIÓN DE LA PERSONA JURÍDICA**”, la misma que tendrá fines eminentemente académicos.

Cuestionario.

1. ¿Qué son los delitos informáticos y cuáles son sus implicaciones?

2. ¿Cuáles son los delitos informáticos previstos en la legislación ecuatoriana?

3. ¿Cuáles son los bienes jurídicos protegidos frente a los delitos informáticos?

4. ¿En qué consiste el ransomware y cuáles son sus implicaciones legales?

5. ¿Las normas penales existentes en Ecuador garantizan una protección eficaz a las personas jurídicas frente a delitos informáticos, como el ransomware?

6. ¿Cuál es su perspectiva sobre la importancia del principio de interpretación en materia penal, especialmente en lo que respecta a los delitos informáticos y el ransomware?

ANEXO 2

UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO



GUÍA DE ENTREVISTA

Fecha: _____

Hora: _____

Lugar (ciudad y sitio específico): _____

Entrevistador: Huerta Morán Estefanía

Entrevistado (a): _____

Introducción: La presente entrevista está dirigida a Jueces Penales, Fiscales, Abogados y Peritos Informáticos de la Ciudad de Riobamba, Provincia de Chimborazo y tiene por objeto recabar información para la realización del Proyecto de Investigación titulado “**LA FALTA DE TIPIFICACIÓN DEL RANSOMWARE Y SU INCIDENCIA EN LA DESPROTECCIÓN DE LA PERSONA JURÍDICA**”, la misma que tendrá fines eminentemente académicos.

Cuestionario.

1. ¿Cuáles son las técnicas comunes utilizadas en los ataques de ransomware y cómo evolucionan con el tiempo?

2. ¿Cómo se investiga un caso de ransomware, incluyendo la identificación de los perpetradores y la recuperación de datos?

3. ¿Qué medidas de seguridad y prevención recomienda para proteger a las personas jurídicas y particulares de los ataques de ransomware?

4. ¿Cuál es la importancia de la recolección y preservación de evidencia digital en casos de delitos informáticos, y cómo se lleva a cabo este proceso?

5. ¿Puede proporcionar ejemplos de casos de ransomware o delitos informáticos que haya investigado o en los que haya proporcionado asesoramiento pericial?

6. ¿Cómo cambian las leyes y regulaciones en materia de delitos informáticos a nivel nacional, y cómo afectan a su trabajo como perito informático?

